LUIGI BIANCHI
PROFESSORE DELLA REGIA UNIVERSITÀ DI PISA

LEZIONI
SULLA
TEORIA DEI NUMERI ALGEBRICI
E PRINCIPI D'ARITMETICA ANALITICA

Corso d'analisi 1920-21 — 2.° Semestre.

PISA
ENRICO SPOERRI, Editore
1921

INDICE.

INTRODUZIONE.

Il campo dei numeri interi di Gauss ed i campi quadratici.

CAPITOLO PRIMO.

Proprietà fondamentali dei numeri algebrici. Corpi algebrici finiti. Numeri interi del corpo. I teoremi di Minkowski sulle forme lineari. Le unità del corpo e la loro determinazione secondo Dirichlet.

CAPITOLO SECONDO.

Ideali nei corpi algebrici. Moltiplicazione e divisibilità degli ideali. Risoluzione unica di un ideale in ideali primi. Congruenze rispetto ad ideali. Equivalenza e classi di ideali. Forme decomponibili coordinate agli ideali. Corpi di Galois.

CAPITOLO TERZO.

Principii di aritmetica analitica. La funzione $\zeta(s)$ di Riemann e la funzione generalizzata $\zeta_K(s)$ di Dedekind per un corpo algebrico $K(\theta)$. Formula di Dedekind pel numero h delle classi. Casi del corpo quadratico e del corpo circolare. Prolungamento analitico della $\zeta(s)$ Riemanniana a tutto il piano complesso. Cenno delle recenti ricerche di *Hecke* sulle proprietà analoghe della $\zeta_K(s)$.

AGGIUNTE.

ERRATA CORRIGE.

Pag. 411. Nella formola (7) linea 2ª, e così alla linea 12ª, nel primo membro della formola: in luogo di

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\frac{1}{n^s} \quad \text{leggasi} \quad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

R. Università di Pisa

Prof: Luigi Bianchi

Lezioni sulla teoria dei numeri algebrici e principi d'aritmetica analitica.

Corso d'analisi 1920-21 = II° Semestre.

Introduzione

Il campo dei numeri interi di Gauss ed i campi quadratici.

§ 1
I numeri interi di Gauss.

La teoria dei numeri ha ricevuto, nel secolo scorso, un'importantissima e considerevole estensione, elevandosi, per opera principalmente di Gauss, Kummer, Dirichlet, Dedekind e Kronecker, ad un'aritmetica generale dei numeri algebrici, o irrazionalità algebriche, cioè di quelle quantità che soddisfano ad equazioni algebriche con ordinarii coefficienti razionali. Il primo passo nella nuova teoria venne fatto da Gauss che trattando, nell'ordinaria aritmetica razionale, dopo la teoria dei residui quadratici, quella dei residui biquadratici, riconobbe la necessità di ampliare il campo degli interi ordinarii in quello dei numeri interi complessi,

cioè della forma $a+ib$ $(i=\sqrt{-1})$, con $\underline{a}$, $\underline{b}$ interi ordinari. Questi numeri $a+ib$ diconsi numeri interi di Gauss e comprendono gli interi ordinarii come i reali fra di essi.

In questo capitolo d'introduzione per numero intero intenderemo senz'altro un intero di Gauss e si aggiungerà l'appellativo di razionale quando per essere $b=0$, si riduce ad un intero ordinario (reale). La totalità di questi interi $a+ib$ è manifestamente un insieme infinito di numeri contenente tutti gli ordinarii interi razionali e che godono della proprietà di riprodursi per le tre prime operazioni elementari: somma, sottrazione e moltiplicazione, e questo si esprime dicendo che essi formano un campo d'integrità, come gli ordinarii numeri interi razionali. Qualunque funzione razionale intera a coefficienti interi ordinarii di quanti si vogliano numeri del campo dà un altro numero del campo.

Dicesi norma di un intero $m=a+ib$, e si indica col simbolo $N(m)$ o Nm, il numero razionale in-

tero e positivo che risulta dal prodotto di m pel suo coniugato $m_0 = a - ib$:

$$Nm = m\, m_0 = a^2 + b^2;$$

questa norma non è altro che il quadrato del modulo $|m|$, cioè $Nm \equiv |m|^2$. Ne risulta subito la proprietà:
La norma di un prodotto di due o più fattori è uguale al prodotto delle norme dei singoli fattori.

Al campo degli interi di Gauss si trasporta facilmente la nozione di divisibilità, colle sue leggi elementari. Si dirà che un intero m è divisibile per un altro n non nullo, quando il quoziente $\frac{m}{n}$ è un altro intero del campo. Ne seguono subito le proprietà elementari:

a) Se l'intero α è divisibile per l'intero β, anche $N(\alpha)$ è divisibile per $N(\beta)$.

E infatti se $\alpha = \beta\gamma$ con γ intero, si ha per quanto precede $N(\alpha) = N(\beta) \cdot N(\gamma)$.

b) Se due interi α, β sono divisibili per un terzo ρ, anche la loro somma, o differenza, è divisibile per ρ.

Infatti da $\alpha = \rho\alpha'$, $\beta = \rho\beta'$, con α', β' interi segue $\alpha \pm \beta = \rho(\alpha' \pm \beta')$

c) Se α è divisibile per β, e β per ρ, è anche α divisibi-

le per ρ.

Da $\alpha = \beta\alpha'$, $\beta = \rho\beta'$ (α', β' interi) segue $\alpha = \rho\cdot(\beta'\alpha')$.

Diciamo unità nel campo di Gauss ogni intero ε che divida 1, e per ciò anche qualunque altro intero. Siccome $N(\varepsilon)$ deve dividere $N(1) = 1$, sarà $N(\varepsilon) = 1$ e viceversa, onde segue:

Nel campo di Gauss esistono quattro e quattro sole unità e sono i numeri

$$\varepsilon = \pm 1 \; , \quad \varepsilon = \pm i \, .$$

È da osservarsi che queste sono, al tempo stesso, le quattro radici quarte dell'unità.

Se due interi α e β sono divisibili scambievolmente l'uno per l'altro, avendosi

$$\frac{\alpha}{\beta} \cdot \frac{\beta}{\alpha} = 1 \, ,$$

il loro quoziente è un'unità, cioè

$$\beta = i^n \alpha \qquad (n = 0, 1, 2, 3) \; ;$$

e viceversa, se differiscono per un fattore unità, si dividono scambievolmente. Due tali interi diconsi associati. I numeri associati si presentano a gruppi di quattro sempre distinti: α, $-\alpha$, $i\alpha$, $-i\alpha$ (salvo quando $\alpha = 0$) e in tutte le questioni di divisibilità si compor-

tato come un unico numero.

Qualunque intero $\underline{\alpha}$ è divisibile per le quattro unità e per i suoi tre numeri associati. Se non esistono altri divisori di α, allora si dirà che $\underline{\alpha}$ è un numero <u>indecomponibile</u>, od anche un numero <u>primo</u>, poichè in questo caso le due nozioni coincidono compiutamente, ciò che più non accade nei casi superiori in generale, come vedremo. Quando $\underline{\alpha}$ non è primo, si dirà un numero composto.

Si osservi subito che il numero 2 primo nel campo reale, è invece composto in quello di Gauss, perchè

$$2=(1+i)(1-i)=-i(1+i)^2,$$

e nessuno dei due fattori $1+i$, $1-i$ è un'unità. Però questi due fattori associati sono essi stessi numeri primi nel campo di Gauss, perchè supposto

$$1+i=\beta\gamma.$$

sarebbe: $N(\beta)N(\gamma)=2$ indi $N(\beta)=1$ $N(\gamma)=2$, ovvero $N(\beta)=2$, $N(\gamma)=1$, sicchè o β o γ, sarebbero unità.

Un intero $a+ib$ dicesi <u>pari</u> quando è divisibile per 2, cioè quando a, b sono ambedue pari. Si dirà che $a+ib$ è <u>semipari</u> quando è divisibile p

$1+i$ ma non per 2, la qual cosa avviene allora soltanto che a, b siano simultaneamente dispari.

Chiameremo infine <u>impari</u> l'intero $a+ib$ se non è divisibile per $1+i$, il che accade quando a, b sono l'uno pari, l'altro impari.

Un numero $m = a+ib$ <u>impari</u> si dirà <u>primario</u> quando sia

$$a \equiv 1 \pmod 4 \quad , \qquad b \equiv 0 \pmod 2 .$$

Facilmente si osserva che in ogni quaderna di interi <u>impari</u> associati ne esiste uno ed uno soltanto primario. Difatti in una tale quaderna

$$a+ib, \quad -b+ia, \quad -a-ib, \quad b-ia$$

due soli hanno la parte reale dispari, e il coefficiente dell'immaginario pari, poniamo p. e.: $a+ib$, $-a-ib$, ed è $a \equiv 1 \pmod 4$ ovvero $-a \equiv 3 \pmod 4$. Nel primo caso è primario $a+ib$, nel secondo $-a-ib$.

§ 2

Algoritmo del massimo comun divisore - Decomposizione in fattori primi.

È noto che nell'aritmetica ordinaria dei numeri reali le leggi per la divisibilità dei numeri, per la loro decomposizione (unica) in fattori primi ecc. possono tutte fondarsi sull'algoritmo euclideo delle successive divisioni per la ricerca del massimo comun divisore di due numeri. Tutte le volte quindi che in un campo d'integrità di numeri vale un algoritmo analogo, sussistono anche le stesse leggi di divisibilità come nell'aritmetica ordinaria, la decomposizione unica in fattori primi ecc. Andiamo ora a stabilire che, in particolare, nel campo dei numeri di Gauss sussiste appunto un tale algoritmo.

Siano α, β due interi complessi qualunque di Gauss, e sia p. e. $N(\alpha) \geq N(\beta)$. Avendosi

$$\frac{\alpha}{\beta} = \frac{\alpha\beta_0}{N(\beta)} \quad (\beta_0 \text{ coniugato di } \beta),$$

se consideriamo l'intero $\alpha\beta_0 = a + ib$ e dividiamo nel modo ordinario $\underline{a}$ e $\underline{b}$ per $N(\beta)$, così però che i resti r, s della divisione siano positivi o negativi

ma in valore assoluto non eccedano $\frac{1}{2} N(\beta)$, potremo scrivere

$$a = N(\beta) a_1 + r \quad , \quad b = N(\beta) . b_1 + s$$

$$r \leq \frac{1}{2} N(\beta) \quad , \quad s \leq \frac{1}{2} N(\beta) ,$$

indi, posto $\rho = a_1 + i b_1$

$$\frac{\alpha}{\beta} = \rho + \frac{r + is}{N(\beta)} ,$$

da cui

$$(1) \qquad \alpha = \beta\rho + \beta_1 \quad , \quad \text{con} \quad \beta_1 = \frac{r + is}{\beta_0} .$$

Ora $\beta_1 = \alpha - \beta\rho$ è intero e per la sua norma $N(\beta_1) = \frac{r^2 + s^2}{N(\beta)}$ (essendo $r \leq \frac{1}{2} N(\beta)$, $s \leq \frac{1}{2} N(\beta)$) vale la disuguaglianza

$$N(\beta_1) \leq \frac{1}{2} N(\beta) .$$

Dunque: dati due interi di Gauss α, β con $N(\alpha) \geq N(\beta)$ si può trovare un altro intero ρ tale che sia $N(\alpha - \beta\rho) \leq \frac{1}{2} N(\beta)$.

Se nella (1) non è $\beta_1 = 0$ (se non è α divisibile per β), si prosegue nel medesimo modo la divisione di β per β_1 e si trovi

$$\beta = \beta_1 \rho_1 + \beta_2 \quad , \quad \text{con} \quad N(\beta_2) \leq \frac{1}{2} N(\beta_1) ,$$

e così si continui. L'operazione avrà certamente un termine con un resto β_n che divida il precedente β_{n-1}, poichè i numeri interi positivi

$$\mathcal{N}(\beta),\ \mathcal{N}(\beta_1),\ \mathcal{N}(\beta_2), \ldots$$

formano una serie decrescente in cui ciascun termine non supera la metà del precedente e per ciò necessariamente si arresta. Se scriviamo la relativa catena limitata di eguaglianze

$$(I)\begin{cases} \alpha = \beta\gamma + \beta_1 , & \mathcal{N}(\beta_1) \leq \frac{1}{2}\mathcal{N}(\beta) \\ \beta = \beta_1\gamma_1 + \beta_2 & \mathcal{N}(\beta_2) \leq \frac{1}{2}\mathcal{N}(\beta_1) \\ \beta_1 = \beta_2\gamma_2 + \beta_3 & \ldots\ldots\ldots \\ \ldots\ldots\ldots & \ldots\ldots\ldots \\ \beta_{n-3} = \beta_{n-2}\gamma_{n-2} + \beta_{n-1} & \ldots\ldots\ldots \\ \beta_{n-2} = \beta_{n-1}\gamma_{n-1} + \beta_n & \mathcal{N}(\beta_n) \leq \frac{1}{2}\mathcal{N}(\beta_{n-1}) , \end{cases}$$

vediamo che ogni divisor comune di α, β divide per la prima anche β_1, indi per la seconda β_2, ecc. e infine β_n. D'altra parte risalendo la catena (I) è chiaro che β_n, dividendo β_{n-1}, divide β_{n-2}, poi β_{n-3}, ... e infine α, β. Dunque β_n è il divisor comune di norma massima di α, β e dicesi per ciò il loro <u>massimo comun divisore</u>; esso può naturalmente venire sostituito da un qualunque dei suoi tre associati. Se questo massimo comun divisore è un'unità, i due numeri α, β diconsi <u>primi fra loro</u>.

Se scriviamo la catena d'eguaglianze (I):

$$\beta_n = \beta_{n-2} - \beta_{n-1}\gamma_{n-1}, \quad \beta_{n-1} = \beta_{n-3} - \beta_{n-2}\gamma_{n-2}, \quad \dots \beta_3 = \beta_1 - \beta_2\gamma_2,$$

$$\beta_2 = \beta - \beta_1\gamma_1, \quad \beta_1 = \alpha - \beta\gamma,$$

eliminando β_{n-1} fra le prime due risulta

$$\beta_n = \beta_{n-2} - \gamma_{n-1}(\beta_{n-3} - \beta_{n-2}\gamma_{n-2}) = (\gamma_{n-1}\gamma_{n-2} + 1)\beta_{n-2} - \gamma_{n-1}\beta_{n-3},$$

cioè β_n è una combinazione lineare, con coefficienti interi di Gauss, di β_{n-2}, β_{n-3}

$$\beta_n = \lambda\beta_{n-2} + \mu\beta_{n-3},$$

quindi anche, a causa di $\beta_{n-2} = \beta_{n-4} - \beta_{n-3}\gamma_{n-3}$, una combinazione lineare di β_{n-3}, β_{n-4}. E così, risalendo, troviamo che β_n è una combinazione lineare di α, β.

Dunque: <u>Se i due interi complessi α, β hanno il massimo comun divisore δ, è risolubile in numeri interi di Gauss ξ, η l'equazione</u>

$$\alpha\xi + \beta\eta = \delta;$$

<u>in particolare</u> se α, β sono primi fra loro, l'altra

$$(1) \qquad \alpha\xi + \beta\eta = 1.$$

Di qui si ha, come corollario, il principio fondamentale per la teoria della divisibilità: <u>Se α, β sono interi primi fra loro e ρ è un terzo intero</u>

qualunque, ogni divisor comune di $\alpha\gamma, \beta$ è anche divisor comune di β, γ. Risoluta infatti in numeri interi ξ, η la (2), si ha

$$\alpha\gamma \cdot \xi + \beta\gamma \cdot \eta = \gamma ,$$

e perciò ogni divisor comune di $\alpha\gamma, \beta$ divide anche γ. In particolare: se un numero β divide il prodotto $\alpha\gamma$ ed è primo col fattore α, divide necessariamente l'altro γ.

Segue di qui (come nel campo reale) la proprietà dei numeri primi nel campo di Gauss: Se un numero primo π divide il prodotto di più numeri interi $\alpha, \beta, \gamma \ldots$, divide almeno due di essi.

Osserviamo ora che, se α è un intero qualunque, ove non sia esso stesso un numero primo, ammetterà almeno un divisore primo. Tale è in ogni caso il divisore π di più piccola norma, perchè se π fosse ulteriormente decomponibile in $\pi = \pi_1 \pi_2$, il divisore π_1 di α avrebbe la norma $N(\pi_1) < N(\pi)$.

Da questi principii fondamentali risulta, come nell'aritmetica ordinaria: Ogni numero intero α di Gauss è risolubile nel prodotto di fattori primi; questa

decomposizione è unica, salvo a sostituire ad uno o più dei fattori primi un suo associato. Per presentare la decomposizione sotto forma unica basterà p.e. convenire che ciascun fattore primo impari di x si assuma sotto forma primaria. Resta ora da rispondere alla questione: Quali sono gli effettivi numeri primi π del campo di Gauss?

Per questo si cominci dall'osservare che qualunque numero intero m di Gauss divide infiniti numeri razionali, almeno $N(m)$ e i suoi multipli, e dimostriamo: Se π è un numero primo nel campo di Gauss, il più piccolo numero reale p divisibile per π è primo nel campo razionale. E infatti se p non fosse primo, risolvendolo in fattori primi $p = q.r \ldots$, il numero primo π, dividendo il prodotto $q.r \ldots$, dividerebbe almeno uno dei fattori, che sarebbe $< p$ contro l'ipotesi. Di qui risulta che, per avere tutti i numeri primi nel campo di Gauss, basta risolvere nei loro fattori primi complessi i numeri primi ordinarii.

Ora, in primo luogo, il numero primo reale 2 dà luogo, come si è visto, all'unico numero primo com-

plesso $1+i$ (o $1-i$), che è semipari. Ogni altro primo π di Gauss è necessariamente impari e se p è il numero primo reale di cui π è divisore, la norma $N(\pi)$ divide $N(p)=p^2$ e non si possono dare che i due casi

$$N(\pi)=p \quad , \quad \text{ovvero} \quad N(\pi)=p^2.$$

Nel primo caso, essendo $p=\pi\,\pi_0$, anche π_0 è un numero primo ma distinto da π, e p è il prodotto di due fattori primi coniugati, ciascuno dei quali dicesi di *1° grado*. In questo caso $p=N(\pi)$ è necessariamente $\equiv 1 \pmod 4$. Nel secondo caso, avendosi

$$N(p)=N(\pi),$$

p e π sono associati e p stesso è un numero primo complesso che si dirà di *2° grado*. Vediamo intanto di qui che: *i numeri primi reali q che sono $\equiv 3 \pmod 4$ restano primi (di 2° grado) anche nel campo di Gauss.*

I numeri primi non reali nel campo di Gauss sono dunque fattori dei numeri primi reali $p\equiv 1 \pmod 4$. Ma sussiste anche la proprietà inversa:

Ogni numero primo reale $p\equiv 1 \pmod 4$ è il prodotto di due fattori coniugati $\pi\,\pi_0$. Questa equivale al noto teorema di Fermat: *ogni numero primo $p\equiv 1 \pmod 4$*

è la somma di due quadrati, che si deduce dai primi teoremi sulle forme quadratiche. Ma a questo punto osserviamo che, senza ricorrere alla teoria delle forme quadratiche, bastano i primi principii ora svolti nel campo di Gauss, in unione per ora al teorema dell'aritmetica reale che, essendo $p \equiv 1 \pmod 4$, -1 è residuo quadratico di p, ossia $\left(\frac{-1}{p}\right) = +1$, per dedurne il teorema di Fermat. Esistendo infatti un numero reale x tale che x^2+1 risulta divisibile per p, possiamo dire che nel campo di Gauss il numero $p \equiv 1 \pmod 4$ divide il prodotto dei due numeri coniugati $(x+i)(x-i)$; e siccome esso non divide manifestamente nessuno dei due fattori, sarà necessariamente decomponibile, in due fattori coniugati, nel campo attuale, ossia $p = a^2 + b^2$. Concludiamo quindi: Nel campo di Gauss i numeri primi sono: 1° gli ordinarii numeri primi reali $q \equiv 3 \pmod 4$, 2° i fattori primi complessi $a+ib$ dei numeri primi reali $p \equiv 1 \pmod 4$, 3° il numero primo $1+i$, al cui quadrato è associato il numero primo ordinario 2.

Facciamo ancora un'ulteriore applicazione di que-

Si risultati alla decomposizione di un numero reale m, che supporremo senz'altro dispari, nella somma di due quadrati $m = a^2 + b^2$ che siano primi fra loro. Scrivendo $m = (a+ib)(a-ib)$, si vede che, nel campo di Gauss, i fattori primi di $a+ib$ (o di $a-ib$) non potranno essere numeri primi reali $q \equiv 3 \pmod 4$, perchè altrimenti q dividerebbe tanto a che b, contro l'ipotesi, e saranno quindi fattori primi complessi. Dunque intanto: condizione necessaria è che m non abbia altri fattori primi che della forma $\equiv 1 \pmod 4$. Si supponga allora m decomposto in fattori primi ordinarii

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

essendo $p_1, p_2, \dots p_r$ tutti diversi fra loro e $\equiv 1 \pmod 4$, e le α gli esponenti a cui figurano in m. Decomponiamo ciascun p nei suoi fattori primi complessi coniugati

$$p_1 = \pi_1 \pi_1', \quad p_2 = \pi_2 \pi_2', \quad \dots p_r = \pi_r \pi_r',$$

ed osserviamo che supposto $m = (a+ib)(a-ib)$ non potrà essere $a+ib$ divisibile ad un tempo per π_1, π_1' chè allora sarebbe anche divisibile per p_1 che entrerebbe come fattore in a e b. Per ciò $a+ib$ sarà divisibi-

te o per $\pi_1^{\alpha_1}$ o per $\pi_1'^{\alpha_1}$, e siccome si passa dall'un caso all'altro cangiando $a+ib$ nel coniugato $a-ib$, si potrà senz'altro supporre che $a+ib$ contenga in fattore $\pi_1^{\alpha_1}$. Allora pel secondo relativo a $p_2^{\alpha_2}$ potremo scegliere a volontà $\pi_2^{\alpha_2}$ ovvero $\pi_2'^{\alpha_2}$, così pel terzo $\pi_3^{\alpha_3}$ o $\pi_3'^{\alpha_3}$, ecc. Si conclude quindi che vi sono 2^{r-1} modi, essenzialmente diversi, per formare $a+ib$, o per decomporre m nella somma di due quadrati primi fra loro. Dunque: Se il numero dispari m contiene r fattori primi diversi, tutti $\equiv 1 \pmod 4$, esso è decomponibile, in 2^{r-1} modi diversi, nella somma di due quadrati primi fra loro.

Esempio $5.13.17=(1+2i)(1-2i).(3+2i)(3-2i).(1+4i)(1-4i)$

$a+ib=(1+2i)(3+2i)(1+4i)$, $a+ib=(1+2i)(3-2i)(1+4i)$

$a+ib=(1+2i)(3+2i)(1-4i)$, $a+ib=(1+2i)(3-2i)(1-4i)$

$1105=5.13.17=33^2+4^2=9^2+32^2=31^2+12^2=23^2+24^2.$

§ 3

Congruenze nel campo di Gauss - Funzione $\Phi(m)$ - Teorema di Fermat.

Se m è un intero di Gauss: $m=a+ib$ ed α, β due

altri interi qualunque del campo si diranno α, β congrui fra loro (mod m), e si scriverà $\alpha \equiv \beta \pmod{m}$, quando la differenza $\alpha - \beta$ sia divisibile per $\underline{m}$. Siccome nel campo d'integrità di Gauss, valgono le stesse leggi fondamentali per la divisibilità come nell'aritmetica ordinaria, così valgono anche gli stessi principii per la teoria delle congruenze, che qui senz'altro saranno applicati.

La prima questione che dobbiamo risolvere è: <u>Dato il modulo m, quanti numeri incongrui esistono (mod m)?</u> - Tutti i numeri $x+iy$ congrui con uno fisso $\alpha + i\beta$, rispetto al modulo $m = a + ib$, hanno la forma

$$x+iy = (a+ib)(t+iu) + \alpha + i\beta,$$

dove t, u percorrono tutti gli interi reali; si ha così

$$\begin{cases} x = at - bu + \alpha \\ y = bt + au + \beta . \end{cases}$$

Sia δ il massimo comun divisore di a, b e dalla seconda sarà y determinato solo (mod δ), onde potremo prendere t, u in guisa che y risulti eguale ad uno dei δ numeri $0, 1, 2, \dots \delta-1$, diciamo

$$y_0 = bt_0 + \alpha u_0 + \beta.$$

Tutte le altre coppie (t, u) che dànno il medesimo valore y_0 ad y sono

$$t = t_0 + \frac{a}{\delta}\rho, \qquad u = u_0 - \frac{b}{\delta}\rho,$$

con ρ intero arbitrario, da cui

$$x = at_0 - bu_0 + \alpha + \frac{a^2+b^2}{\delta}\rho,$$

ossia

$$x = x_0 + \frac{N(m)}{\delta}\rho \qquad (x_0 = at_0 - bu_0 + \alpha).$$

Dunque x è determinato solo rispetto al modulo $\frac{N(m)}{\delta}$, e disponendo di t, u (cioè di ρ), si può fare x eguale al minimo resto positivo di x_0 (mod $\frac{N(m)}{\delta}$). Dunque y_0 percorre δ valori distinti ed x ne percorre $\frac{N(m)}{\delta}$, onde si conclude: Rispetto al modulo $m = a + ib$ esistono, nel campo di Gauss, precisamente $N(m) = \delta.\frac{N(m)}{\delta}$ numeri incongrui. - In particolare si osservi che, se a, b sono primi fra loro, cioè $\delta = 1$, si può prendere $y_0 = 0$ e formano un sistema completo di resti (mod $a + ib$), gli interi reali

$$0, 1, 2, \ldots N(m) - 1.$$

Siano ora A, B due interi fissi di Gauss, dei quali A sia primo col modulo m, e nel binomio $Ax + B$

si faccia percorrere ad x un sistema completo di resti (un sistema di $N(m)$ numeri incongrui (mod m)); allora anche $Ax+B$ percorrerà un sistema completo di resti. E infatti se $Ax+B \equiv Ax'+B \pmod{m}$, si ha $A(x'-x) \equiv 0 \pmod{m}$ ed essendo m primo con A dividerà $x'-x$. In particolare ne risulta che una sola volta riuscirà $Ax+B \equiv 0 \pmod{m}$, cioè:

La congruenza lineare $Ax+B \equiv 0 \pmod{m}$, se A è primo col modulo m possiede una ed una sola radice. Questo vale in particolare se il modulo m è un numero primo π, che non divide A.

Indichi ora $f(x)$ un polinomio in x di grado n

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n ,$$

i cui coefficienti $a_0, a_1, \dots a_n$ sono interi di Gauss, dei quali il primo a_0 non sia divisibile pel numero primo π, e dimostreremo come nell'aritmetica ordinaria:

La congruenza di grado n rispetto al modulo primo π

$$(1) \qquad f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \equiv 0 \pmod{\pi} \qquad a_0 \not\equiv 0 \pmod{\pi}$$

possiede al massimo n radici incongrue. La proprietà sussiste, come si è visto, per $n=1$ e basterà provare

che se è vera per le congruenze di grado $n-1$, è vera anche per quelle di grado n. E invero sia α una prima radice della (1), e si divida nel modo ordinario $f(x)$ per $x-\alpha$, onde avremo

$$(2) \qquad f(x) = (x-\alpha) f_1(x) + f(\alpha)$$

con $f_1(x)$ di grado $n-1$ e primo coefficiente $= a_0$. Siccome $f(\alpha) \equiv 0 \pmod{\pi}$ si ha identicamente per qualunque x

$$f(x) \equiv (x-\alpha) f_1(x) \qquad (\text{mod } \pi),$$

ed ogni ulteriore radice β di $f(x) \equiv 0$, distinta da α, risulta radice di $f_1(x) \equiv 0$. Se dunque la prima avesse più di n radici incongrue, la seconda ne avrebbe più di $n-1$, contro l'ipotesi.

Suppongasi ora che la (1) abbia in effetto n radici incongrue e d'altra parte si abbia $f(x) = \varphi(x) . \psi(x)$, con $\varphi(x)$, $\psi(x)$ polinomi della stessa specie di $f(x)$, e di grado r, s rispettivamente con $r+s=n$; dimostriamo: <u>ciascuna delle congruenze</u>

$$(3) \qquad \varphi(x) \equiv 0 \pmod{\pi}, \qquad \psi(x) \equiv 0 \pmod{\pi}$$

<u>ha precisamente tante radici quante unità il grado, e cioè r la prima, s la seconda.</u>

Difatti se α è una qualunque radice di $f(x) \equiv 0$, avendo

dosi $\varphi(\alpha).\psi(\alpha) \equiv 0 \pmod{\pi}$ il numero primo π dividerà o $\varphi(\alpha)$ o $\psi(\alpha)$, e sarà dunque α radice di una (almeno) delle congruenze (3). Sia r' il numero delle radici della prima, s' quello della seconda e però $r' \leq r$, $s' \leq s$. La proposta avrà al massimo $r'+s'$ radici, e poichè ne ha in effetto $n = r+s$, sarà necessariamente $r' = r$, $s' = s$.

La funzione $\Phi(m)$ di Gauss. – Fra gli $N(m)$ numeri incongrui (mod m), ve ne saranno alcuni primi con m; indichiamone il numero con $\Phi(m)$ e cerchiamo la espressione di questa funzione numerica. E in primo luogo dimostriamo: Se m si scinde nel prodotto di r fattori primi fra loro due a due:

$$m = m_1 . m_2 \dots m_r ,$$

si ha

$$\Phi(m) = \Phi(m_1) . \Phi(m_2) \dots \Phi(m_r) .$$

Cominciamo dal provare che dati, rispetto ai moduli $m_1, m_2, \dots m_r$, r numeri arbitrarii $\beta_1, \beta_2, \dots \beta_r$, esiste sempre (mod m) uno ed un solo numero x, che soddisfi alle congruenze

$$(4) \qquad x \equiv \beta_1 \pmod{m_1}, \quad x \equiv \beta_2 \pmod{m_2}, \dots x \equiv \beta_r \pmod{m_r}.$$

Per ciò, come nell'aritmetica ordinaria, prendiamo

r numeri (di Gauss) che soddisfino alle rispettive congruenze

$$\frac{m}{m_1} x_1 \equiv 1 \pmod{m_1}, \quad \frac{m}{m_2} x_2 \equiv 1 \pmod{m_2}, \ldots \frac{m}{m_r} x_r \equiv 1 \pmod{m_r},$$

e pongasi

$$(5) \qquad x \equiv \frac{m}{m_1} x_1 \beta_1 + \frac{m}{m_2} x_2 \beta_2 + \cdots + \frac{m}{m_r} x_r \beta_r \pmod{m},$$

onde le (4) saranno manifestamente soddisfatte. D'altra parte se x' è un secondo numero che soddisfa le (4), la differenza $x'-x$ è divisibile per $m_1, m_2, \ldots m_r$ e quindi anche pel loro prodotto m, cioè $x' \equiv x \pmod{m}$.

Ora si osserva subito nella (5) che x risulta primo con m, allora ed allora soltanto che β_1 sia primo con m_1, β_2 con m_2, $\ldots \beta_r$ con m_r e per ciò appunto

$$\Phi(m) = \Phi(m_1) . \Phi(m_2) \ldots \Phi(m_r), \quad \text{c. d. d.}$$

Ciò premesso, basterà saper calcolare $\Phi(m)$ quando m è una potenza π^n di un numero primo π. Ora, per trovare i $\Phi(\pi^n)$ numeri non divisibili per π, dobbiamo togliere dai $N(\pi^n)$ di un sistema completo di resti (mod π^n) quelli divisibili per π, e questi divisi per π danno un sistema completo di resti (mod π^{n-1}), e sono quindi in numero di $N(\pi^{n-1})$. Difatti se A, B sono divisibili per π ed incongrui (mod π^n), i due $\frac{A}{\pi}$, $\frac{B}{\pi}$ sono incon-

grui (mod π^{n-1}) e viceversa. Ne deduciamo dunque

$$\Phi(\pi^n) = N(\pi^n) - N(\pi^{n-1}) = N(\pi^n)\left(1 - \frac{1}{N(\pi)}\right),$$

ed in generale, se $\pi_1, \pi_2, \ldots \pi_r$ sono i fattori primi distinti di m, l'espressione effettiva della funzione numerica $\Phi(m)$ sarà

$$(A) \quad \Phi(m) = N(m)\left(1 - \frac{1}{N(\pi_1)}\right)\left(1 - \frac{1}{N(\pi_2)}\right) \cdots \cdots \left(1 - \frac{1}{N(\pi_r)}\right).$$

Veniamo ora al teorema di Fermat nel campo di Gauss, e supposto che A sia un intero primo col modulo m, nel binomio Ax facciamo percorrere a x i $\Phi(m)$ numeri incongrui $x_1, x_2, \ldots x_{\Phi(m)}$ di un sistema completo di resti primi con m. I numeri

$$Ax_1, \; Ax_2, \; \ldots \ldots Ax_{\Phi(m)}$$

saranno tutti primi con m e incongrui fra loro, e perciò congrui, in altro ordine con $x_1, x_2, \ldots x_{\Phi(m)}$. Facendone il prodotto, risulta

$$A^{\Phi(m)} \cdot X \equiv X \pmod{m}, \quad X = x_1, x_2, \ldots x_{\Phi(m)},$$

e siccome X è primo con m, dividendo risulta il teorema di Fermat generalizzato

$$A^{\Phi(m)} \equiv 1 \pmod{m},$$

che vale adunque se A è primo col modulo m. In particolare se m è un numero primo π, ed A è un nume-

ro non divisibile per π, si avrà

$$A^{N(\pi)-1} \equiv 1 \pmod{\pi};$$

in ogni caso per A qualunque

$$A^{N(\pi)} \equiv A \pmod{\pi}.$$

§ 4

Resti di potenze - Radici primitive (mod π) - Tabelle d'indici.

Dimostriamo ora rapidamente come al campo di Gauss si estendano i risultati dell'aritmetica ordinaria pei resti di potenze, le radici primitive rispetto ad un modulo primo π, ecc., e vedremo poi in seguito che questo è soltanto un primo caso d'estensione all'aritmetica generale dei numeri (corpi) algebrici.

Sia A un intero (di Gauss), primo col modulo $\underline{m}$, e consideriamo (mod m) la serie delle successive potenze

$$A^0 = 1 \quad , \quad A, A^2, A^3, \ldots\ldots$$

La prima a riprodursi (mod m) è la $A^0 = 1$, e se δ è il minimo esponente (positivo) pel quale ciò avviene diremo che A appartiene (mod m) all'esponente δ, onde

le potenze $(1, A, A^2, \ldots A^{\delta-1})$ sono incongrue fra loro (mod m).
Precisamente come nel campo reale, si dimostrano le proprietà seguenti:

α) La condizione necessaria e sufficiente perchè sia $A^r \equiv A^s \pmod{m}$ è che si abbia $r \equiv s \pmod{\delta}$. In particolare è $A^r \equiv 1 \pmod{\delta}$ solo quando $r \equiv 0 \pmod{\delta}$; e siccome, pel teorema di Fermat, $A^{\Phi(m)} \equiv 1 \pmod{m}$: l'esponente δ cui appartiene A è in ogni caso un divisore di $\Phi(m)$.

β) Se A appartiene all'esponente δ, una potenza A^r di A appartiene all'esponente $\frac{\delta}{\varepsilon}$, essendo ε il massimo comune divisore di r, δ.

γ) Se i due numeri A, A' appartengono ad esponenti δ, δ' primi fra loro, il loro prodotto AA' appartiene all'esponente prodotto $\delta\delta'$. Sia d l'esponente cui appartiene AA', indi $(AA')^d \equiv 1 \pmod{m}$. Introducendo il numero reciproco A_1 di A, tale cioè che $AA_1 \equiv 1 \pmod{m}$, e che appartiene manifestamente allo stesso δ, la precedente può scriversi

$$A'^{d} \equiv A_1^{d}$$

e siccome A' appartiene a δ' ed A_1 a δ, il numero a sinistra appartiene per la β) a un divisore di δ', quello eguale a destra a un divisore di δ, cioè essendo δ,

δ' primi fra loro, si ha

$$A'^{d} \equiv 1 \quad , \quad A_1^{d} \equiv 1$$

e per ciò $\underline{d}$ è multiplo comune di δ, δ' indi di $\delta\delta'$. Ma sic come $(AA')^{\delta\delta'} \equiv 1 \pmod{m}$, se ne conclude che necessariamente $d = \delta\delta'$.

δ) Consideriamo i $\Phi(m)$ numeri A primi con m; ciascuno di essi appartiene ad un esponente divisore di $\Phi(m)$ ed ora dimostriamo: <u>Se d è il massimo di questi esponenti, ogni altro δ è un divisore di d.</u> Suppongasi che A appartenga al <u>massimo</u> esponente d, e, se è possibile, A' appartenga ad un esponente $\underline{\delta}$ non divisore di $\underline{d}$. Esisterà dunque in δ un fattore primo p almeno che entrerà in δ ad una potenza maggiore che non in $\underline{d}$, sia p.e. alla potenza p^{r+s} in δ, alla potenza p^s in d, ove $r>0$, $s \geq 0$. Poniamo

$$\delta = p^{r+s}.\delta_1 , \qquad d = p^s.d_1 ,$$

ove δ_1, d_1 non sono più divisibili per p. A causa della β) il numero $A'^{\delta_1} = a'$ appartiene all'esponente p^{r+s}, e l'altro $A^{p^s} = a$ all'esponente d_1, primo con p^{r+s}. Il prodotto $a'a$ apparterrebbe dunque all'esponente $p^{r+s}d_1 > d$, contro la ipotesi che $\underline{d}$ sia il massimo.

Tutte queste proprietà valgono per un modulo m composto qualunque. Ma supponiamo ora che il modulo sia un numero primo π, e dimostriamo come ne segue l'esistenza di radici primitive $g \pmod{\pi}$, cioè di numeri g appartenenti all'esponente (di Fermat) $N(\pi)-1 = \Phi(\pi)$. Bisognerà provare che, nel caso attuale, il massimo esponente, sopra indicato con d, è appunto $=\Phi(\pi)$. Qualunque dei $\Phi(\pi)$ numeri x, non divisibili per π, appartiene ad un esponente divisore di d, ed è per ciò in ogni caso

$$x^d \equiv 1 \pmod{\pi}.$$

Questa congruenza ha per ciò, rispetto al modulo primo π, $\Phi(\pi)$ radici incongrue, e il suo grado d non può dunque, pel § 3, essere inferiore a $\Phi(\pi)$; d'altronde d è, per la α), un divisore di $\Phi(\pi)$, da cui appunto $d = \Phi(\pi)$.

Dimostrata così l'esistenza di radici primitive g rispetto ad ogni modulo primo π nel campo di Gauss, ne risulta come nell'aritmetica ordinaria che le sue potenze

$$g^0 = 1, \quad g, g^2, \dots g^{\Phi(\pi)-1}$$

danno tutti i $\Phi(\pi)$ numeri possibili $\pmod{\pi}$, e si estende quindi immediatamente al campo di Gauss la teoria de-

gli indici e tutte le sue conseguenze.

Si osservi poi che se il numero primo (impari) π è complesso (di 1° grado), $N(\pi) = p$ è un numero primo ordinario $\equiv 1 \pmod 4$ ed il sistema completo di resti $(\bmod p)$

$$1, 2, 3, \ldots p-1$$

dà anche un sistema completo di resti $(\bmod \pi)$; in questo caso le radici primitive reali $(\bmod p)$ sono anche radici primitive nel campo di Gauss.

Se si tratta invece di un numero primo π di 2° grado, cioè di un numero primo reale $q \equiv 3 \pmod 4$, si avrà un sistema completo di resti $(\bmod q)$ dal numero $\alpha + i\beta$ facendo percorrere ad α, β i valori $0, 1, 2, \ldots q-1$ esclusa la combinazione $(0, 0)$. P. e. se prendiamo $\pi = 7$, una radice primitiva è $g = 1 + 2i$ ed è $\Phi(\pi) = 48$. Elevando g alle successive potenze $0, 1, 2, \ldots 47$ e calcolando i successivi resti, possiamo formare la tabella seguente:

(6)	12	46	13	41	23	19	10
(5)	44	7	30	3	45	42	25
(4)	4	11	33	38	2	15	5
(3)	28	29	39	26	14	9	35
(2)	20	1	18	21	27	6	31
(1)	36	34	43	47	17	37	22
(0)	*	0	32	40	16	8	24
	(0)	(1)	(2)	(3)	(4)	(5)	(6)

Per trovare l'indice di un numero $\alpha + i\beta$ dove $\alpha, \beta = 0, 1, 2, 3, 4, 5, 6$ si osservi la casella all'incrocio della verticale segnata inferiormente con (α) colla orizzontale segnata lateralmente a sinistra con (β); in questa casella è segnato l'indice del numero; così p.e. $\text{ind}(3+5i) = 3$, $\text{ind}(4+i) = 17$, ecc. L'uso di queste tabelle è analogo a quelle dell'aritmetica reale. Così p.e. volendo risolvere la congruenza lineare:

$$(5+3i)X \equiv 3+i \pmod 7,$$

si calcoli $\text{ind}(3+i) = 47$, $\text{ind}(5+3i) = 9$, da cui $X = 47 - 9 = 38$, $X \equiv 3+4i$. Si osserverà che, scindendo il reale dall'immaginario, ciò equivale a risolvere nell'aritmetica reale il sistema delle due congruenze lineari in due incognite ξ, η

$$\begin{cases} 5\xi - 3\eta \equiv 3 \\ 3\xi + 5\eta \equiv 1 \end{cases} \pmod 7$$

Come altro esempio si voglia riconoscere se è solubile la congruenza quadratica

$$X^2 \equiv 4 + 3i \pmod 7$$

e trovare le (due) radici. Prendendo gli indici risulta

$$2\,\text{ind}\,X \equiv \text{ind}(4+3i) \equiv 14 \pmod{48}$$

e la cosa è possibile perchè l'indice è pari. Ne risultano

i due valori

$$\text{ind}\, X = 7, \qquad \text{ind}\, X = 31,$$

e però le due radici $X \equiv 1+5i$, $6+2i$ $(\text{o} \; -(1+5i))$.

§ 5.

Residui quadratici - Simbolo $\left[\frac{D}{\pi}\right]$ di Dirichlet.

Se π è un numero primo (impari) nel campo di Gauss, e D un numero qualunque non divisibile per π, si dirà che D è residuo quadratico di π, se è solubile la congruenza: $x^2 \equiv D \pmod{\pi}$, e invece non residuo se la congruenza è impossibile.

Dirichlet ha introdotto, per significare il carattere quadratico di D rispetto al numero primo π, il simbolo (analogo a quello di Legendre)

$$\left[\frac{D}{\pi}\right],$$

al quale attribuisce il valore $+1$ se D è residuo, il valore -1 se è non residuo.

Ora prendiamo un sistema completo di resti $(\text{mod}\, \pi)$, escluso lo zero, e siano

$$\mu_1, \mu_2, \dots \mu_r \qquad r = \Phi(\pi) = N(\pi) - 1$$

diciamo associati due numeri μ, siano μ_i, μ_k quando si ha

$$\mu_i \mu_k \equiv \mathcal{D} \pmod{\pi}.$$

Così ogni numero μ ha il suo associato, e se dapprima supponiamo $\mathcal{D}$ non residuo, le coppie di numeri associati constano sempre di numeri μ distinti; e poichè il prodotto dei numeri in ciascuna coppia è $\equiv \mathcal{D} \pmod{\pi}$, ne risulta

$$(1) \qquad \mu_1 \mu_2 \ldots \mu_r \equiv \mathcal{D}^{\frac{N(\pi)-1}{2}} \pmod{\pi}, \quad \text{se} \left[\frac{\mathcal{D}}{\pi}\right] = -1$$

Quando invece $\mathcal{D}$ è residuo, la congruenza $x^2 \equiv \mathcal{D} \pmod{\pi}$ ha due e due sole radici e fra i numeri $\mu_1, \mu_2, \ldots \mu_r$ se ne hanno due soli $\mu, -\mu$ ciascuno dei quali coincide col proprio associato ed il loro prodotto è $= -\mu^2 \equiv -\mathcal{D} \pmod{\pi}$; perciò

$$(2) \qquad \mu_1 \mu_2 \ldots \mu_r \equiv -\mathcal{D}^{\frac{N(\pi)-1}{2}} \pmod{\pi}, \quad \text{se} \left[\frac{\mathcal{D}}{\pi}\right] = 1.$$

Siccome $\mathcal{D} = 1$ è certamente residuo, si deduce dalla (2) il teorema (di Wilson)

$$\mu_1 \mu_2 \ldots \mu_r \equiv -1 \pmod{\pi}$$

e le (1), (2) danno rispettivamente

$$\left.\begin{array}{l} \mathcal{D}^{\frac{N(\pi)-1}{2}} \equiv -1 \\ \mathcal{D}^{\frac{N(\pi)-1}{2}} \equiv 1 \end{array}\right\} \pmod{\pi} \quad \begin{array}{l} \text{se} \left[\frac{\mathcal{D}}{\pi}\right] = -1 \\ \text{se} \left[\frac{\mathcal{D}}{\pi}\right] = +1 \end{array}$$

risultato analogo a quello d'Eulero pel campo reale, e che si compendia nella formola

$$\left[\frac{\mathfrak{D}}{\pi}\right] \equiv \mathfrak{D}^{\frac{N(\pi)-1}{2}} \pmod{\pi}.$$

È facile vedere che le proprietà del simbolo di Legendre si mantengono nel simbolo di Dirichlet, in particolare le due fondamentali

$$\left[\frac{A}{\pi}\right] = \left[\frac{B}{\pi}\right], \quad \text{se} \quad A \equiv B \pmod{\pi}$$

$$\left[\frac{ABC\ldots}{\pi}\right] = \left[\frac{A}{\pi}\right]\left[\frac{B}{\pi}\right]\left[\frac{C}{\pi}\right]\cdots$$

Del resto Dirichlet stesso ha ridotto il calcolo del suo simbolo $\left[\frac{\mathfrak{D}}{\pi}\right]$ nell'aritmetica di Gauss a quello di Legendre nell'aritmetica reale, o al generalizzato di Jacobi, colle considerazioni seguenti:

a) Sia dapprima π un numero primo reale $q \equiv 3 \pmod 4$ e pongasi $\mathfrak{D} = \alpha + i\beta$. Se è solubile la congruenza

$$(3) \qquad X^2 \equiv \alpha + i\beta \pmod q,$$

scindendo X nella parte reale e immaginaria col porre $X = t + iu$, sarà solubile, in aritmetica reale, il sistema

$$(4) \qquad \begin{cases} t^2 - u^2 \equiv \alpha \\ 2tu \equiv \beta \end{cases} \pmod q;$$

e viceversa se questo è solubile, sarà solubile la (3). Ma dalle (4) deduciamo

$$(t^2 + u^2)^2 \equiv \alpha^2 + \beta^2 \pmod q,$$

onde vediamo che se

$$(5)\qquad \left[\frac{\alpha+i\beta}{q}\right]=+1$$

si ha anche

$$(6)\qquad \left(\frac{\alpha^2+\beta^2}{q}\right)=+1.$$

Inversamente proviamo che dalla (6) segue la (5). Sia dapprima $\alpha=0$, e il sistema (4) diventerà

$$u\equiv\pm t\,,\qquad 2t^2\equiv\pm\beta\pmod q$$

e siccome $\left(\frac{-1}{q}\right)=-1$ si può sempre soddisfare alla seconda congruenza scegliendo una delle due determinazioni di segno.

Se poi $\alpha\not\equiv 0\pmod q$, sussistendo per ipotesi la (6), si può trovare un numero s tale che

$$s^2\equiv\alpha^2+\beta^2\pmod q,$$

ossia

$$(s-\beta)(s+\beta)\equiv\alpha^2\pmod q,$$

onde risulta

$$\left(\frac{s-\beta}{q}\right)=\left(\frac{s+\beta}{q}\right)=\pm 1\,.$$

Ma possiamo sempre supporre che valga il segno superiore, bastando nel caso contrario sostituire $-s$ a s. Dopo ciò prendiamo due interi φ,ψ tali che si abbia

$$\varphi^2\equiv s+\beta\,,\quad \psi^2\equiv s-\beta\pmod q,$$

ed avremo dunque

$$\varphi^2\psi^2\equiv\alpha^2\pmod q,$$

indi

$$\varphi\psi \equiv \pm \alpha \pmod q.$$

Inoltre potremo assumere φ, ψ tutti due dispari o tutti due pari, e allora i numeri interi

$$t = \frac{\varphi \pm \psi}{2}, \quad u = \frac{\varphi \mp \psi}{2}$$

verificheranno le (4). Così il simbolo di Dirichlet $\left[\frac{\alpha + i\beta}{\pi}\right]$ per π reale $\equiv 3 \pmod 4$ si riduce a quello di Legendre col la formula

$$(I) \qquad \left[\frac{\alpha + i\beta}{q}\right] = \left(\frac{\alpha^2 + \beta^2}{q}\right), \quad o \quad \left[\frac{m}{q}\right] = \left(\frac{N(m)}{q}\right)$$

b) Sia ora $\pi = a + ib$ un numero complesso di 1° grado, che sarà lecito supporre scritto sotto forma primaria (§ 1), con a dispari, b pari; sarà in tal caso

$$N(\pi) = a^2 + b^2 = p,$$

con p numero primo $\equiv 1 \pmod 4$. Per ridurre anche in questo caso il calcolo del simbolo di Dirichlet $\left[\frac{\alpha + i\beta}{a + ib}\right]$ a quello di un simbolo di Legendre, cominciamo dall'osservare che se $\alpha + i\beta$ è residuo di $\pi = a + ib$, sarà solubile la congruenza

$$x^2 \equiv \alpha + i\beta \pmod \pi$$

e a questa si potrà soddisfare con <u>x reale</u> (§ 3) perchè a, b sono primi fra loro, onde potremo porre

$$x^2 = \alpha + i\beta + (a+ib)(t+iu)$$

con t, u reali. Ne deduciamo

$$\begin{cases} at - bu = x^2 - \alpha \\ bt + au = -\beta \end{cases}$$

e risolvendo rapporto a t, u (essendo $p = a^2 + b^2$):

$$\begin{cases} pt = a(x^2 - \alpha) - b\beta \\ pu = -b(x^2 - \alpha) - a\beta. \end{cases}$$

È dunque necessario e sufficiente che x soddisfi alle due congruenze simultanee reali

$$\begin{cases} a\,x^2 \equiv a\alpha + b\beta \\ b\,x^2 \equiv b\alpha - a\beta, \end{cases} \pmod p$$

delle quali però la seconda p. e., a causa dell'identità

$$a(ax^2 - a\alpha - b\beta) + b(bx^2 - b\alpha + a\beta) = p(x^2 - \alpha),$$

è una conseguenza della prima. Quest'identità prova anche che non può essere $a\alpha + b\beta \equiv 0 \pmod p$, altrimenti sarebbe anche $b\alpha - a\beta \equiv 0 \pmod p$, onde

$$\alpha + i\beta = (a+ib)\left(\frac{a\alpha+b\beta}{p} + i\,\frac{b\alpha - a\beta}{p}\right)$$

sarebbe divisibile per π contro l'ipotesi. Dunque, affinchè sia $\alpha + i\beta$ residuo di π, è necessario e sufficiente che sia solubile la congruenza

$$a\,x^2 \equiv a\alpha + b\beta \pmod p,$$

cioè che si abbia

$$\left(\frac{a}{p}\right) = \left(\frac{a\alpha + b\beta}{p}\right).$$

D'altra parte avendosi $p = a^2 + b^2$, indi $p \equiv b^2 \pmod{a}$ il simbolo di Jacobi $\left(\frac{p}{a}\right)$ ha il valore $+1$ e quindi, pel teorema ordinario di reciprocità, è anche $\left(\frac{a}{p}\right) = +1$. Se ne conclude che sarà $\left[\frac{\alpha + i\beta}{a + ib}\right] = +1$ allora ed allora soltanto quando si abbia

$$\left(\frac{a\alpha + b\beta}{p}\right) = +1.$$

Ne risulta la seconda formola di Dirichlet

$$(II) \qquad \left[\frac{\alpha + i\beta}{a + ib}\right] = \left(\frac{a\alpha + b\beta}{p}\right),$$

che raggiunge lo scopo prefisso.

§ 6

Il teorema di reciprocità nel campo di Gauss.

Il secondo problema della teoria dei residui quadratici, che consiste nel trovare di quali numeri primi impari π è residuo un dato numero D, si riduce essenzialmente ai tre casi elementari

$$D = i, \quad D = 1 + i, \quad D = \alpha + \beta i,$$

essendo $\alpha + \beta i$ un numero primo impari, che assumeremo sempre sotto la forma primaria. Basterà dunque saper calcolare successivamente i valori dei sim-

boli

$$1)\ \left[\frac{i}{\pi}\right],\quad 2)\left[\frac{1+i}{\pi}\right],\quad 3)\left[\frac{\alpha+\beta i}{\pi}\right],$$

dove $\pi = a+ib$ è un numero primo impari, che si assumerà ancora sotto la forma primaria.

1) Il valore del simbolo $\left[\frac{i}{\pi}\right]$ si ricava immediatamente dal criterio d'Eulero (§ 5)

$$\left[\frac{i}{\pi}\right] \equiv i^{\frac{N(\pi)-1}{2}} \quad (\mathrm{mod}\ \pi),$$

onde risulta subito la formula

$$(III) \qquad \left[\frac{i}{\pi}\right] = (-1)^{\frac{N(\pi)-1}{4}}$$

2) Riguardo al simbolo $\left[\frac{1+i}{\pi}\right]$, sia $\pi = a+ib$ reale o complesso, proviamo che sussiste sempre la formula

$$(IV) \qquad \left[\frac{1+i}{a+ib}\right] = (-1)^{\frac{(a+b)^2-1}{8}}.$$

Sia dapprima $a+ib$ reale $= -q \equiv 1 \ (\mathrm{mod}\ 4)$. Dalla (I) si ha

$$\left[\frac{1+i}{q}\right] = \left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}},$$

che coincide colla (IV).

Se poi $a+ib$ è complesso (primario), e $p = a^2+b^2$, sarà per la

$$(II) \qquad \left[\frac{1+i}{a+ib}\right] = \left(\frac{a+b}{p}\right).$$

Ma avendosi $2p = (a+b)^2 + (a-b)^2$, risulta

$$2p \equiv (a-b)^2 \quad (\mathrm{mod}\ a+b)$$

e, adoperando il simbolo di Jacobi e il teorema di reciprocità:

$$\left(\frac{2}{a+b}\right) = \left(\frac{p}{a+b}\right) = \left(\frac{a+b}{p}\right),$$

indi

$$\left(\frac{a+b}{p}\right) = (-1)^{\frac{(a+b)^2-1}{8}}, \quad \text{cioè la (IV).}$$

3) Per il calcolo del simbolo $\left[\frac{\alpha+i\beta}{a+ib}\right]$ serve, come nel campo reale, il teorema di reciprocità, che assume qui la forma semplice

$$\text{(V)} \qquad \left[\frac{\alpha+i\beta}{a+ib}\right] = \left[\frac{a+ib}{\alpha+i\beta}\right].$$

Suddistinguiamo tre casi possibili:

a) se i due numeri primi $\alpha+i\beta$, $a+ib$ sono tutti due reali, la (V) si riduce alla

$$\left[\frac{\alpha}{a}\right] = \left[\frac{a}{\alpha}\right],$$

ed in effetto per la (I) i due simboli a destra e sinistra hanno il valore $+1$.

b) Sia ora $\alpha+i\beta$ reale $=-q\equiv 1 \pmod 4$ e $a+ib$ complesso con $p=a^2+b^2\equiv 1 \pmod 4$.

La (V) si riduce a

$$\left[\frac{q}{a+ib}\right] = \left[\frac{a+ib}{q}\right],$$

che si tratta di verificare. In effetto, per la (I), è

$$\left[\frac{a+ib}{q}\right] = \left[\frac{a^2+b^2}{q}\right] = \left(\frac{p}{q}\right),$$

e per la (II)

$$\left[\frac{q}{a+ib}\right] = \left(\frac{aq}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right),$$

perchè come si è visto sopra $\left(\frac{a}{p}\right) = +1$. Per l'ordinario teorema di reciprocità è $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ e la (V) è provata in questo caso.

c) Se infine $a+ib$, $\alpha+i\beta$ sono ambedue complessi (primarii) pongasi

$$a^2+b^2=p\ ;\quad \alpha^2+\beta^2=P$$

con p, P numeri primi reali $\equiv 1 \pmod 4$. Si ha per la (II)

$$\left[\frac{\alpha+i\beta}{a+ib}\right]=\left(\frac{a\alpha+b\beta}{p}\right),\qquad \left[\frac{a+ib}{\alpha+i\beta}\right]=\left(\frac{a\alpha+b\beta}{P}\right).$$

Ora essendo

$$(a\alpha+b\beta)^2+(b\alpha-a\beta)^2=pP$$

ed $a\alpha+b\beta$ impari ne segue $pP\equiv(b\alpha-a\beta)^2 \pmod{a\alpha+b\beta}$, indi

$$\left(\frac{p}{a\alpha+b\beta}\right)=\left(\frac{P}{a\alpha+b\beta}\right),$$

e perciò anche (pel teorema ordinario di reciprocità)

$$\left(\frac{a\alpha+b\beta}{p}\right)=\left(\frac{a\alpha+b\beta}{P}\right),$$

il che dimostra la formola (V) anche in quest'ultimo caso.

§ 7

Estensione a nuovi campi quadratici - Il primo esempio della separazione fra numeri indecomponibili e fattori primi.

Le considerazioni svolte nei paragrafi precedenti possono ripetersi, senza nuove difficoltà, per alcuni altri campi quadratici, dando luogo alle stesse conseguenze fondamentali della decomponibilità essenzialmente unica di ogni intero del campo in un prodotto di fattori primi. Dopo il campo introdotto da Gauss per lo studio dei residui biquadratici, venne considerato da Jacobi e Eisenstein, il campo d'integrità determinato dalla radice cubica θ dell'unità

$$\theta = \frac{-1+i\sqrt{3}}{2},$$

che si presenta nella teoria dei residui cubici. In questo campo gli interi sono della forma $a+b\theta$ con a, b interi ordinarii; essi si riproducono per somma, sottrazione e moltiplicazione e comprendono tutti gli interi ordinarii, onde formano ancora un campo d'integrità. I concetti e le prime proprietà della divisibilità valgono ancora qui, e così pure quello di norma

$$N(a+b\theta)=(a+b\theta)(a+b\theta^2)=a^2-ab+b^2=(a-b)^2+ab$$

(a causa di $\theta^2+\theta+1=0$, $\theta^3=1$); esistono nel campo le 6 sole unità (di norma $=1$)

$$\pm 1,\ \pm\theta,\ \pm\theta^2.$$

In modo perfettamente analogo a quello descritto al §1, si vede che, nel caso attuale, vale ancora un algoritmo del massimo comun divisore, giacchè se α, β sono due interi qualunque del campo e $N(\alpha) \geq N(\beta)$, determinando convenientemente un intero ρ, si può far sì che risulti $N(\alpha-\beta\rho) < N(\beta)$. Dopo ciò valgono gli stessi principii fondamentali per la divisibilità come al §2, la decomponibilità unica nel prodotto dei fattori primi ecc. Altri corpi quadratici in cui vale ancora un algoritmo delle divisioni successive per la ricerca del massimo comun divisore di due numeri, sono quelli dei campi d'integrità della forma $a+b\theta$ (a, b interi ordinarii) dove θ è una radice dell'equazione quadratica

$$\theta^2+\theta+2=0,\quad \theta^2+2=0,\quad \theta^2+\theta+3=0 \quad \text{(corpi immaginarii)}$$

$$\theta^2+\theta-1=0,\quad \theta^2-2=0,\quad \theta^2-3=0,\quad \theta^2+\theta-3=0 \quad \text{(corpi reali)}$$

E sebbene negli ultimi quattro campi (corpi reali)

esistano infinite unità, la circostanza che sussiste sempre un algoritmo analogo a quello d'Euclide fa sì che valgono nel campo tutte le leggi ordinarie della divisibilità, e in particolare chiamando <u>indecomponibile</u> nel campo ogni numero che non può risolversi nel prodotto di due fattori ciascuno dei quali sia diverso da un'unità, ne risulta che: <u>Ogni numero indecomponibile nel campo si comporta come un effettivo numero primo, cioè non può dividere il prodotto di due fattori senza dividere uno almeno di essi</u>.

E qui osserviamo subito che sebbene l'esistenza di un algoritmo euclideo sia condizione sufficiente per la identità fra i numeri indecomponibili ed i fattori primi, nel senso ora spiegato, non è del resto necessaria. Così nel campo quadratico (immaginario) $a + b\theta$ con $\theta^2 + \theta + 5 = 0$ non vale un algoritmo euclideo, ma tutti i numeri indecomponibili si comportano ancora come numeri primi.

Ma passiamo ora a descrivere, in un primo e più semplice esempio, il nuovo fenomeno della <u>separazione fra numeri indecomponibili e fattori primi</u>, che si è

presentato a Kummer nello studio di quei campi di numeri che nascono dal problema della divisione del cerchio, studio che ha dato luogo alla geniale creazione di Kummer della teoria degli ideali.

Si consideri il campo quadratico immaginario relativo alla equazione $\theta^2+5=0$, cioè gli interi quadratici della forma

$$\alpha = a + i b \sqrt{5} \qquad (a, b \text{ interi ordinari}).$$

Le prime osservazioni del § 1 sulla divisibilità dei numeri, e sulle loro norme, valgono ancora in questo campo, dove esistono le due sole unità ± 1, poichè l'equazione $a^2+5b^2=1$ non ammette altre soluzioni in interi che $a=\pm 1$, $b=0$. Un numero α di questo campo è certamente indecomponibile se non sono solubili in numeri interi ordinarii x, y le equazioni

$$x^2+5y^2=\delta,$$

dove δ percorrerà i divisori (puri) di $N(\alpha)=a^2+5b^2$. Così i quattro numeri

$$2, \quad 3, \quad 1+\theta=1+i\sqrt{5}, \quad 1-\theta=1-i\sqrt{5}$$

sono indecomponibili, poichè le loro norme sono

$$N(2)=4, \qquad N(3)=9 \quad, N(1+\theta)=N(1-\theta)=6$$

e le equazioni

$$x^2+5y^2=2\,, \quad x^2+5y^2=3$$

non ammettono soluzioni intere. Ora, avendoci

$$6 = 2.3 = (1+\theta)(1-\theta),$$

si vede che il numero indecomponibile 2 (o 3) divide il prodotto dei due fattori $(1+\theta)$, $(1-\theta)$ senza dividere alcuno dei due. A questo fenomeno è congiunto l'altro sopra descritto che il numero 6 consente due decomposizioni distinte nel prodotto di due fattori, ciascuno dei quali è indecomponibile. Analogamente sono indecomponibili i numeri 7, $1+2i\sqrt{5}$, $1-2i\sqrt{5}$, e si ha

$$21 = 3.7 = (1+2i\sqrt{5})(1-2i\sqrt{5}).$$

Le difficoltà descritte in questo caso più semplice si ripetono in quasi tutti gli altri campi quadratici, e tanto più nei superiori, onde sembrava opera vana il cercare di ripristinare, in tutti i casi, le leggi ordinarie della divisibilità e della decomposizione unica in fattori primi. Questo scopo, come già sopra si è detto, venne raggiunto da Kummer, nel campo dei numeri delle radici n^{me} dell'unità, colla creazione dei suoi numeri *ideali*, che non esistono propriamente nel corpo ma vengo-

no ad esso aggregati (aggiunti). È merito principale
? del Dedekind (e del Kronecker che raggiunse lo scopo
analogo per altra via) di avere estesa la teoria di Kummer a <u>tutti</u> i corpi algebrici, sostituendo in pari tempo
alla nozione dei fattori ideali di Kummer quella di sistemi di infiniti numeri, <u>effettivamente esistenti nel corpo</u>,
che portano il nome di <u>ideali</u>.

Sarà utile, prima di esporre i principii dell'aritmetica
generale dei corpi algebrici, di spiegare la nozione fondamentale di <u>ideali</u>, secondo Dedikind, sugli esempî più
semplici considerati fin qui.

Prendiamo uno qualunque dei campi d'integrità
trattati, sia il campo razionale ordinario, o il campo
di Gauss o i varii campi quadratici sopra discussi.

Scegliamo un intero qualunque α del campo e consideriamo tutti i multipli di α. Questi costituiscono
un sistema J infinito di interi del campo, nel quale
si riconoscono subito le proprietà seguenti:

a) <u>La somma o la differenza di due numeri di J è sempre un numero di J.</u>

b) <u>Il prodotto di ogni numero di J per un qualunque nu-</u>

mero del campo d'integrità è ancora un numero di I.

Chiamiamo ideale del campo d'integrità ogni sistema (infinito) di numeri del campo che goda delle due proprietà a) e b). L'ideale I si dice principale se consta, come quelli sopra costruiti, di tutti i numeri del campo divisibili per un numero fondamentale α, ma in generale esistono anche ideali non principali o secondarii. È appunto il fenomeno sopra notato, che nei campi generali l'indecomponibilità di un numero non assicura il suo funzionamento come fattore primo è indissolubilmente legato all'esistenza di ideali non principali. Così è facile vedere che, nei campi pei quali vale l'algoritmo delle successive divisioni, ogni ideale I è principale. Infatti, se si considera dapprima il caso di un ideale I nel campo dei numeri interi reali, è immediatamente visibile che, se n è il più piccolo di questi (in valore assoluto), tutti gli altri sono multipli di n, ed ogni ideale è quindi principale. Lo stesso dicasi per un ideale I nel campo di Gauss $a+ib$, di cui tutti i numeri sono necessariamente multipli di quello di più piccola norma; e così pure dicasi per gli altri

campi nei quali sussiste l'algoritmo delle divisioni.

Ma prendiamo invece il campo $a + ib\sqrt{5}$ nel quale abbiamo riscontrato il nuovo fenomeno e consideriamo in questo p.e. l'insieme di quei numeri pei quali $a \equiv b \pmod 2$. Essi formano, come subito si vede, un ideale J, essendo soddisfatte le condizioni a) b). Questo ideale J contiene in particolare tutti i multipli di 2, cioè comprende l'ideale principale generato dal numero 2, ma non è un ideale principale perchè se esso constasse dei multipli di un numero α, la norma $N(\alpha)$ dovrebbe dividere le norme di tutti i numeri di J e però anche $N(2)=4$, $N(1+i\sqrt{5})=6$ e sarebbe quindi $N(\alpha)=2$, ciò che è assurdo. Similmente formano un altro ideale non principale quei numeri $a+ib\sqrt{5}$ nei quali $a \equiv b \pmod 3$, il quale contiene in particolare tutti i multipli di 3.

Colla introduzione degli ideali e colle successive nozioni di prodotti di ideali, di divisibilità degli ideali ecc. viene resa possibile, come si vedrà, la costruzione di un'aritmetica generale dei corpi algebrici, governata dalle stesse semplici leggi che vigono nell'aritmetica ordinaria.

Capitolo I

Proprietà fondamentali dei numeri algebrici - Corpi algebrici - Teoremi di Minkowski sulle forme lineari - Le unità del corpo e la loro determinazione secondo Dirichlet.

§ 8

Polinomi a coefficienti razionali.

I polinomi in una variabile x che avremo da considerare nel seguito saranno quasi sempre funzioni razionali intere della x con coefficienti numeri razionali, e questa condizione s'intenderà sempre tacitamente ammessa, salvo dichiarazione contraria.

Dagli elementi dell'algebra (calcolo letterale) ricordiamo le proprietà fondamentali seguenti. Se $f(x)$, $\varphi(x)$ sono due polinomi dei rispettivi gradi m, n ed è $m \geq n$, la divisione ordinaria di $f(x)$ per $\varphi(x)$ porge (in modo unico)

$$(1) \qquad f(x) = q(x)\varphi(x) + r_1(x),$$

dove il polinomio $q(x)$ (quoziente) è di grado $m-n$ e l'altro $r_1(x)$ (resto) di grado $\leq n-1$. Se il resto $r_1(x)$ è identicamente nullo, allora $\varphi(x)$ divide $f(x)$.

Dalla (1) segue che ogni polinomio $g(x)$ il quale divida simultaneamente $f(x)$, $\varphi(x)$ divide anche $(\varphi(x)\,;\, r_1(x))$ ed inversamente. Su questa osservazione è basata la ricerca del <u>massimo comun divisore</u> di due polinomi $f(x)$, $\varphi(x)$ per la catena delle divisioni successive

$$(a)\quad \begin{cases} f(x) = q(x)\,\varphi(x) + r_1(x) \\ \varphi(x) = q_1(x)\, r_1(x) + r_2(x) \\ r_1(x) = q_2(x)\, r_2(x) + r_3(x) \\ \dots\dots\dots\dots \\ r_{s-2}(x) = q_{s-1}(x)\, r_{s-1}(x) + r_s(x)\,, \end{cases}$$

dove l'ultimo resto $r_s(x)$ (che divide il precedente $r_{s-1}(x)$) rappresenta appunto il massimo comun divisore di $f(x)$, $\varphi(x)$. Risalendo per questa catena d'eguaglianze risulta

$$r_s(x) = A(x)\, f(x) + B(x)\,\varphi(x)$$

dove $A(x)$, $B(x)$ sono due polinomi. Il massimo comun divisore $d(x) = r_s(x)$ è il polinomio di minimo grado pel quale sussiste un'identità della forma

$$(b)\qquad d(x) = A(x)\, f(x) + B(x)\,\varphi(x).$$

Se il massimo comun divisore $d(x)$ di $f(x)$, $\varphi(x)$ è una costante (un numero razionale) i due polinomi $f(x)$, $\varphi(x)$ diconsi primi fra loro. Radici di un polinomio $f(x)$ chiamiamo le radici dell'equazione $f(x)=0$. Ogni eventuale radice comune di $f(x)$, $\varphi(x)$ è, per la (b), anche radice di $d(x)$, e viceversa; non esistono radici comuni se i polinomi sono primi fra loro.

Un polinomio $f(x)$ si dice riducibile se può decomporsi nel prodotto di due effettivi polinomi $f_1(x)$, $f_2(x)$ (non costanti)

$$f(x) = f_1(x)\, f_2(x);$$

altrimenti si dirà irriducibile. Un processo dovuto a Kronecker permette sempre di constatare, con un numero finito di operazioni, se un polinomio dato $f(x)$ è irriducibile o riducibile.

Sussiste ora la proprietà fondamentale: se il polinomio $f(x)$ è irriducibile e un altro polinomio $G(x)$ ha una radice comune con $f(x)$, ammette tutte le sue radici ed è $G(x)$ divisibile per $f(x)$. Si consideri infatti il massimo comun divisore $d(x)$ di $f(x)$, $G(x)$, che non sarà una costante non nulla, annullandosi per la radice comune irriducibile, e coincide quindi, salvo un fattore costan-

te, con $f(x)$.

Segue di qui in particolare che un polinomio irriducibile $f(x)$ non può avere radici comuni con un polinomio di grado minore, e quindi anche non può ammettere radici multiple, che sarebbero comuni al polinomio derivato $f'(x)$.

Quando un polinomio <u>irriducibile</u> $f(x)$ divide il prodotto $A(x).B(x)$ di due altri polinomi $A(x), B(x)$, dividerà almeno uno di essi, poichè avrà almeno con uno di questi una radice comune. Ne segue che la decomposizione di un polinomio riducibile $F(x)$ nel prodotto di polinomi irriducibili

$$F(x) = f_1(x) \cdot f_2(x) \cdots f_r(x)$$

è essenzialmente unica, salvo che si possono moltiplicare $f_1(x), f_2(x) \ldots f_r(x)$ per fattori costanti (razionali) $c_1, c_2, \ldots c_r$ così che sia $c_1 c_2, \ldots c_r = 1$.

Il più delle volte variando i nostri polinomi per fattori costanti si potranno rendere con primo coefficiente $=1$ e gli altri numeri razionali; ovvero si potranno rendere tutti i coefficienti interi

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

e senza divisore comune. In questo caso il polinomio $f(x)$ si dirà primitivo.

§ 9

Prime proprietà dei numeri algebrici.

Chiamasi numero algebrico ogni numero θ, reale o complesso, che sia radice di un polinomio $f(x)$ a coefficienti razionali. E qui potremo supporre che il primo coefficiente di $f(x)$ sia $= 1$, ovvero che siano tutti, a cominciare dal primo, numeri razionali interi senza divisore comune. Naturalmente, dato un numero algebrico θ, vi sono infinite equazioni algebriche a cui soddisfa, ma fra queste ve ne sarà una di minimo grado, la quale sarà necessariamente irriducibile (§ 8). È chiaro che ogni numero razionale a è anche da considerarsi come algebrico, perchè soddisfa all'equazione lineare $x - a = 0$.

Dicesi grado di un numero algebrico θ il grado n dell'equazione irriducibile $f(x) = 0$ a cui soddisfa; e così i numeri algebrici di 1° grado sono i numeri razionali.

Un numero algebrico θ, di grado n individua perfettamente n numeri algebrici $\theta_1, \theta_2, \dots \theta_n$ tutti diversi fra loro,

e cioè le radici di $f(x)=0$. Questi si dicono i numeri algebri-ci coniugati di θ_1, ed uno qualunque di essi appartiene al medesimo polinomio irriducibile $f(x)$ e individua tutti gli $n-1$ rimanenti. Per non confondere questa denominazione di numeri coniugati di θ coll'ordinaria nozione di numero complesso coniugato, converremo di aggiungere, in questo secondo caso, l'appellativo di complesso coniugato di θ, che si indicherà con θ_0 ovvero con $\bar{\theta}$. Per l'insieme dei numeri algebrici coniugati si userà, oltre la notazione $\theta_1\ \theta_2 \dots \theta_n$ anche l'altra $(\theta', \theta'', \dots \theta^{(n)})$ ovvero $(\theta, \theta', \theta'', \dots \theta^{(n-1)})$. Si osservi anche che, se un polinomio $\Phi(x)$ si annulla per $x=\theta$, si annulla anche per qualunque coniugato $x=\theta^{(r)}$, perchè risulta $\Phi(x)$ divisibile per $f(x)$ (§ 8).

Veniamo ora alla nozione fondamentale di numero intero algebrico:

Ogni numero θ che soddisfi ad un'equazione

$$(1) \qquad g(x) = x^m + b_1 x^{m-1} + b_2 x^{m-2} e \dots + b_{m-1} x + b_m = 0$$

con primo coefficiente $=1$, e gli altri razionali interi, dicesi un intero algebrico.

Vedremo fra breve che, se θ è un intero algebrico, anche l'equazione (irriducibile) di grado minimo a cui θ

soddisfa, scritta col primo coefficiente $=1$, ha gli altri coefficienti razionali interi. Un numero algebrico non intero si dirà frazionario. Si osservi però che se il numero algebrico θ soddisfa ad un'equazione (1) coi numeri b razionali frazionarii, sarebbe erroneo dedurne che θ sia necessariamente frazionario, perchè può benissimo esistere un'altra equazione (1) colle b numeri interi a cui θ ancora soddisfa. [Così p.e. l'intero algebrico $\sqrt{5}$ soddisfa all'equazione con coefficienti frazionari $x^3+\frac{1}{5}x^2-5x-1=0$].

È chiaro che un numero intero ordinario N (razionale) è anche un intero algebrico, come radice dell'equazione $x-N=0$; ma importa anche osservare, per assicurarsi che il nuovo concetto di numero intero non può trovarsi in contradizione coll'antico, che: Ogni numero intero algebrico e che sia razionale è un intero ordinario. Suppongasi infatti $\theta=\frac{p}{q}$ con p, q interi ordinarii primi fra loro. Sostituendo nella (1) e moltiplicando per q^{m-1} segue

$$\frac{p^m}{q}=-\left\{b_1 p^{m-1}+b_2 q p^{m-2}+\cdots\cdots+b_{m-1} p q^{m-2}+b_m q^{m-1}\right\}.$$

Il numero a destra è un intero ordinario, indi quello a sinistra; ma essendo q primo con p, indi con p^m, è necessariamente $q=1$.

D'ora innanzi per numero intero intenderemo senz'altro un intero algebrico e vi aggiungeremo l'appellativo di razionale, quando si tratti di un intero ordinario. Se θ è un numero intero (algebrico), esso soddisfa ad una equazione come la (1), e a questa soddisfano anche, per quanto precede, i suoi coniugati, i quali sono perciò interi; dunque:

a) Se θ è un intero (algebrico), tutti i suoi coniugati sono interi.

Sia ora θ un qualunque numero algebrico, e sia

$$a_0\theta^m + a_1\theta^{m-1} + \dots + a_{m-1}\theta + a_m = 0$$

un'equazione algebrica a coefficienti razionali interi a cui soddisfa. Il numero $\theta' = a_0\theta$ soddisfa all'equazione

$$\theta'^m + a_1\theta'^{m-1} + a_2 a_0 \theta'^{m-2} + \dots + a_m a_0^{m-1} = 0,$$

con primo coefficiente $=1$, e gli altri razionali interi, quindi θ' è un intero algebrico.

Si ha dunque il teorema:

b) Se θ è un numero algebrico, si può ridurre intero moltiplicandolo per un conveniente numero razionale intero (e positivo) r.

Per stabilire le ulteriori proprietà dei numeri algebri-

ci, è utile premettere il seguente:

Lemma c) Sia θ un numero complesso, e suppongasi che esistano r numeri (complessi) $\xi_1, \xi_2, \dots \xi_r$ non tutti nulli, pei quali sussistano le r relazioni

$$(2)\quad \begin{cases} \theta \xi_1 = c_{11}\xi_1 + c_{12}\xi_2 + \cdots\cdots + c_{1r}\xi_r \\ \theta \xi_2 = c_{21}\xi_1 + c_{22}\xi_2 + \cdots\cdots + c_{2r}\xi_r \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \theta \xi_r = c_{r1}\xi_1 + c_{r2}\xi_2 + \cdots\cdots + c_{rr}\xi_r \end{cases},$$

con coefficienti c_{ik} razionali. In tal caso il numero θ è algebrico di grado r al massimo, e se di più i coefficienti c_{ik} sono razionali interi, allora θ è intero algebrico.

E infatti l'eliminazione delle ξ fra le (2) dà per θ l'equazione di grado r in θ

$$\begin{vmatrix} c_{11}-\theta, & c_{12} & \cdots & c_{1r} \\ c_{21} & c_{22}-\theta & \cdots & c_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ c_{r1} & c_{r2} & \cdots & c_{rr}-\theta \end{vmatrix} = 0$$

con primo coefficiente $=(-1)^r$ e gli altri razionali, anzi interi, se tali sono i coefficienti c_{ik}.

Ciò posto, è facile dimostrare il teorema:

d) <u>La somma, la differenza e il prodotto di due numeri algebrici α, β sono ancora numeri algebrici (medesimamente il quoziente $\frac{\alpha}{\beta}$ $(\beta \neq 0)$); se di più α e β sono interi, anche $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ sono interi.</u>

Se α, β sono dei rispettivi gradi n, m e le equazioni irriducibili che li definiscono si scrivono

$$\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n = 0$$

$$\beta^m + b_1\beta^{m-1} + b_2\beta^{m-2} + \cdots + b_m = 0,$$

colle a, b numeri razionali, pongasi $r = mn$, e prendansi i numeri $\xi_1, \xi_2, \ldots \xi_r$ eguali, in un ordine qualunque, agli $mn = r$ numeri

$$1, \alpha, \alpha^2 \ldots \alpha^{n-1}; \beta, \alpha\beta, \ldots \alpha^{n-1}\beta; \beta^{m-1}, \beta^{m-1}\alpha, \beta^{m-1}\alpha^2, \ldots \beta^{m-1}\alpha^{n-1},$$

ossia $\xi = \alpha^p\beta^q$, $0 \leq p < n$, $0 \leq q < m$. Il numero $\alpha\xi = \alpha^{p+1}\beta^q$ è un altro numero ξ se $p < n-1$, mentre se $p = n-1$

$$\alpha\xi = -\beta^q(a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots a_n,$$

ossia $\alpha\xi$ è una combinazione lineare dei numeri ξ a <u>coefficienti razionali</u> se tali sono i coefficienti $\underline{a}$, e più particolarmente interi quando sono interi gli $\underline{a}$. Analoga osservazione vale per un $\beta\xi$, quindi si ha anche

$$(\alpha \pm \beta)\xi_j = c_{j1}\xi_1 + c_{j2}\xi_2 + \cdots c_{jr}\xi_r$$

dove i coefficienti c_i sono in generale razionali e di più interi, se tali sono i coefficienti a_i, b_k. Siccome poi i numeri ξ non sono nulli, applicando il lemma, si vede che $\alpha \pm \beta$ è algebrico, anzi intero se α, β sono interi. Lo stesso vale manifestamente pel prodotto $\alpha\beta$ e il teorema d) è dimostrato. [Per il quoziente $\frac{\alpha}{\beta}$ si osservi che $\frac{1}{\beta}$ è algebrico con β].

Combinando questi risultati elementari, si ha l'altro generale: Ogni funzione razionale intera a coefficienti interi (razionali) di un numero qualunque di variabili diventa un intero algebrico se per queste variabili si sostituiscono dei valori che siano interi algebrici.

Ritornando ora sulla definizione di numero intero algebrico, data al principio del §, è da osservarsi che la $g(x)$ può anche essere riducibile, ma in ogni caso:

L'equazione irriducibile a cui soddisfa l'intero θ, scritta col primo coefficiente $= 1$, avrà gli altri coefficienti interi. E infatti questi coefficienti eguagliano le funzioni simmetriche elementari delle radici,

che sono tutte interi algebrici, e però i coefficienti stessi sono interi (razionali).. Risulta anche di qui la proprietà (Gauss) che se un polinomio $F(x)$ con primo coefficiente $=1$ e gli altri interi, è riducibile, i polinomi irriducibili in cui si decompone, scritti con primo coefficiente $=1$ avranno tutti gli altri coefficienti interi.

§ 10

Ulteriori proprietà degli interi algebrici.

Per i numeri interi algebrici, in generale, vale una più ampia proprietà di riproduzione che non per gli interi ordinari (razionali), contenuta nel teorema:

α) Ogni radice θ di un'equazione

$$\theta^n + \alpha\,\theta^{n-1} + \beta\,\theta^{n-2} + \cdots + \rho = 0$$

con primo coefficiente $=1$ e gli altri interi (algebrici) è ancora un intero algebrico.

Siano

$$\alpha^{n_1} + a_1\alpha^{n_1-1} + \cdots\; a_{n_1} = 0$$

$$\beta^{n_2} + b_1\beta^{n_2-1} + \cdots\; b_{n_2} = 0$$

$$\cdots\cdots\cdots\cdots$$

$$\rho^{n_s} + c_1\rho^{n_s-1} + \cdots\; c_{n_s} = 0$$

le equazioni dei rispettivi gradi $n_1, n_2 \dots$ che definiscono $\alpha, \beta, \dots$, i coefficienti a, b, c essendo razionali interi. Poniamo $r = n_1 n_2 \dots n_s n$ e in un ordine qualunque

$$\xi_1, \xi_2, \dots \xi_n = \alpha^{s_1} \beta^{s_2} \dots \theta^t \qquad \text{con } 0 \leq s_1 < n_1, \quad 0 \leq s_2 < n_2, \dots 0 \leq t < n$$

Si vede subito che $\theta \xi$ è una combinazione lineare a coefficienti interi di $\xi_1, \xi_2, \dots \xi_r$, ed applicando il lemma c), ne risulta che θ è un intero algebrico c.d.d.

Dal teorema α) deduciamo ora il seguente corollario:

β) <u>Se</u> $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \dots + \alpha_{n-1} x + \alpha_n$ <u>è un polinomio a coefficienti α algebrici interi e θ è una sua radice, il numero $\alpha_0 \theta$ è intero.</u> E infatti, posto $v = \alpha_0 \theta$, abbiamo

$$v^n + \alpha_1 v^{n-1} + \alpha_2 \alpha_0 v^{n-2} + \dots + \alpha_n \alpha_0^{n-1} = 0,$$

onde, pel teorema α), il numero v è intero.

Consideriamo ora il polinomio $\frac{f(x)}{x-\theta} = \beta_0 x^{n-1} + \beta_1 x^{n-2} + \beta_2 x^{n-3} + \dots + \beta_{n-1}$ che si ottiene dividendo $f(x)$ pel binomio $x - \theta$ e dimostriamo che anche tutti i coefficienti β sono interi.

Siccome per $n=1$ la proprietà è evidente (essendo allora $f(x) = \alpha_0 (x - \theta)$), basterà provare che se è vero per un polinomio di grado $\leq n-1$, sussiste anche pel grado n.

Ora il polinomio

$$f(x) - \alpha_0 x^{n-1} (x - \theta) = \varphi(x)$$

ha grado $\leq n-1$ e coefficienti interi per β) ed ammette la radice θ onde per la nostra ipotesi, avremo

$$\varphi(x) = (x-\theta)\,\psi(x),$$

con $\psi(x)$ a coefficienti interi. Ne risulta

$$f(x) = (x-\theta)\left[\alpha_0 x^{n-1} + \psi(x)\right],$$

e i coefficienti $\beta_0, \beta_1, \dots \beta_{n-1}$ sono in effetto interi.

Dopo ciò possiamo estendere il teorema β) nel seguente:

γ) Se il polinomio $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \dots + \alpha_{n-1} x + \alpha_n$ ha coefficienti (algebrici) interi e $\theta_1, \theta_2, \dots \theta_r$ sono sue radici (ciascuna al massimo ripetuta secondo l'ordine di moltiplicità) il numero $\alpha_0 \theta_1 \theta_2 \dots \theta_r$ è un intero.

Dall'identità

$$f(x) = \alpha_0 (x-\theta_1)(x-\theta_2) \dots (x-\theta_r)(x-\theta_{r-1}) \dots (x-\theta_r),$$

applicando ripetutamente il risultato precedente, segue che hanno coefficienti interi i successivi polinomi.

$$\frac{f(x)}{x-\theta_n},\ \frac{f(x)}{(x-\theta_n)(x-\theta_{n-1})},\ \dots\ \frac{f(x)}{(x-\theta_n)(x-\theta_{n-1})(x-\theta_{r+1})} = \alpha_0 (x-\theta_1)(x-\theta_2)\cdots(x-\theta_r)$$

Ora il termine costante nell'ultimo è $(-1)^r \alpha_0 \theta_1 \theta_2 \cdots \theta_r$.

Come nell'aritmetica ordinaria, diciamo un intero (algebrico) α divisibile per un altro intero $\beta \neq 0$, o β un divisore di α, se il numero $\frac{\alpha}{\beta}$ è intero, e siccome i numeri interi si riproducono per somma, sottrazione e

moltiplicazione valgono anche qui le leggi elementari:
1) un numero intero β che divide più interi $\alpha_1, \alpha_2, \alpha_r$ divide anche la loro somma 2) se l'intero α è divisibile per β, e questo per l'intero ρ, anche α è divisibile per ρ.

Ciò premesso dal teorema ρ) ne deduciamo un altro di importanza fondamentale per il seguito che si enuncia:

δ) Se due polinomi $A(x)$, $B(x)$

$$A(x) = \alpha_0 x^m + \alpha_1 x^{m-1} + \dots + \alpha_m$$

$$B(x) = \beta_0 x^n + \beta_1 x^{n-1} + \dots + \beta_n$$

hanno coefficienti interi (algebrici) e nel loro prodotto

$$C(x) = A(x) B(x) = \rho_0 x^{m+n} + \rho_1 x^{m+n-1} + \dots + \rho_{m+n}$$

tutti i coefficienti (necessariamente interi) $\rho_0, \rho_1, \dots \rho_{m+n}$ sono divisibili per uno stesso numero intero ν, allora anche ogni prodotto $\alpha_i \beta_k$ $(i = 0, 1, \dots m,\ k = 1, 2, \dots n)$ è divisibile per ν.

Nel caso che $A(x)$ o $B(x)$ si riduca ad una costante la proprietà è evidente e per ciò supponiamo $m > 0$, $n > 0$. Risolvendo $A(x)$, $B(x)$ nei loro fattori lineari abbiasi

$$A(x) = \alpha_0 (x - \xi_1)(x - \xi_2) \dots (x - \xi_m)$$

$$B(x) = \beta_0 (x - \eta_1)(x - \eta_2) \dots (x - \eta_n),$$

e sarà quindi per ipotesi

$$\frac{A(x)\,B(x)}{\nu} = \frac{\alpha_0 \beta_0}{\nu} \Pi(x-\xi)\,\Pi(x-\eta)$$

un polinomio a coefficienti interi. Dunque, pel teorema β), un qualunque prodotto

$$\frac{\alpha_0 \beta_0}{\nu} \xi' \xi'' \ldots \eta' \eta'' \ldots,$$

con un numero qualunque di ξ, e un numero qualunque di η, sarà un intero. Ora $\frac{\alpha_i}{\alpha_0}$ e $\frac{\beta_k}{\beta_0}$, come funzioni simmetriche elementari le prime delle ξ, le seconde delle η, hanno la forma

$$\frac{\alpha_i}{\alpha_0} = \pm \Sigma \xi' \xi'' \ldots, \qquad \frac{\beta_k}{\beta_0} = \pm \Sigma \eta' \eta'' \ldots$$

Moltiplicando risulta

$$\frac{\alpha_i \beta_k}{\nu} = \Sigma \pm \frac{\alpha_0 \beta_0}{\nu} \xi' \xi'' \ldots \eta' \eta'' \ldots$$

e i termini della somma a destra, per l'osservazione precedente, sono tutti interi, per ciò anche $\frac{\alpha_i \beta_k}{\nu}$ c. d. d.

§ 11

Corpi di numeri algebrici – Corpi finiti.

Un sistema di (infiniti) numeri di specie qualunque

$$\alpha, \beta, \rho \ldots$$

che si riproducono mediante le operazioni razionali, dicesi un campo di razionalità (Kronecker). Basta per ciò che le operazioni elementari di somma, sottrazione,

moltiplicazione e divisione (esclusa la divisione per zero), applicate a due numeri qualunque del campo, diano di nuovo un numero del campo, ed allora qualunque funzione razionale a <u>coefficienti razionali</u> di un numero qualunque di essi dà nuovamente un numero del campo. Nel seguito, in luogo della denominazione campo di razionalità, adotteremo l'altra più breve di <u>corpo</u> (Dedekind). In ogni corpo, insieme ad un suo numero $\alpha \neq 0$, è contenuto per definizione l'altro $\frac{\alpha}{\alpha} = 1$, per ciò anche ogni numero intero positivo o negativo, e insieme qualunque numero razionale. La totalità dei numeri razionali è manifestamente un corpo, ed il più piccolo possibile, come contenuto in qualunque altro corpo.

Limitando le nostre considerazioni ai corpi di numeri <u>algebrici</u> è chiaro, per le proprietà fondamentali dei numeri algebrici (§ 9), che la totalità dei numeri algebrici costituisce appunto un corpo ed il più ampio possibile. In questo corpo i numeri interi, riproducendosi per somma, sottrazione e moltiplicazione, formano un campo d'integrità. Esaminiamo ora come si comportano in questo campo totale i numeri interi riguardo al-

la loro divisibilità, decomponibilità in fattori ecc. Per questo dobbiamo porre la nozione fondamentale di unità, indicando con questo nome qualunque numero intero algebrico ε che divide 1, cioè tale che anche $\frac{1}{\varepsilon}$ sia un intero, indi anche un'unità. È chiaro che esistono nel corpo totale dei numeri algebrici infinite unità e tali sono le radici delle equazioni a coefficienti interi con primo ed ultimo coefficiente $= 1$. Le unità si riproducono manifestamente per moltiplicazione, divisione ed estrazione di radice. Ogni unità ε divide qualunque intero α, giacchè $\frac{\alpha}{\varepsilon} = \frac{1}{\varepsilon} \cdot \alpha$ è anche intero. Due numeri interi α, β non nulli divisibili l'uno per l'altro differiscono solo per un fattore unità, perchè $\frac{\alpha}{\beta} \cdot \frac{\beta}{\alpha} = 1$. Due tali numeri si dicono associati, e si comportano nel medesimo modo riguardo alla divisibilità per altri numeri.

Ne segue che ogni intero α è divisibile per infiniti numeri, e cioè per le unità e per tutti i suoi numeri associati, ed è quindi sempre decomponibile, in infiniti modi, nel prodotto di interi. Si sarebbe quindi indotti a riguardare come numeri essenzialmente indecomponibili soltanto quelli che non ammettono al-

tri divisori, oltre le unità ed i numeri associati. Ma è facile vedere che, nel campo totale dei numeri algebrici, non esistono di siffatti numeri indecomponibili ed ha sempre luogo per ogni numero una decomponibilità essenziale illimitata. Basta per questo ricorrere al teorema fondamentale del § precedente ed osservare che, se α è un intero qualunque, diverso da un'unità, anche

$$\sqrt{\alpha}\ ,\ \sqrt[3]{\alpha}\ , \ldots$$

sono interi algebrici, divisori di α, senza essere unità, e così abbiamo p.e. la decomposizione essenziale $\alpha = \sqrt{\alpha}.\sqrt{\alpha}$, ecc.

Invece di considerare il campo totale dei numeri algebrici, conviene quindi limitarsi a campi infinitamente più ristretti, come quello dei numeri razionali, dei numeri di Gauss, ecc. per poter ristabilire in questi le leggi fondamentali dell'aritmetica. Ciò si ottiene restringendosi ai così detti <u>corpi finiti</u>, la cui nozione stabiliamo nel modo seguente. Abbiasi un corpo K di numeri algebrici, e prendiamo dal corpo r numeri qualunque

$$\omega_1\ ,\ \omega_2\ , \ldots \omega_r\ ;$$

noi diremo che gli r numeri ω_i sono linearmente indipendenti se non sussiste alcuna uguaglianza della forma

$$c_1\omega_1 + c_2\omega_2 + \cdots + c_r\omega_r = 0$$

colle c numeri razionali, che si potranno anche supporre, ove esistano, interi primi fra loro: <u>Un corpo algebrico K si dirà finito, e precisamente di grado n, se esistono nel corpo n numeri indipendenti, mentre invece $n+1$ numeri del corpo sono sempre linearmente legati.</u>

Daremo nel prossimo paragrafo la costruzione effettiva (che sarà insieme la più generale) di un corpo algebrico di grado n. Qui cominciamo dall'osservare che se θ è un numero qualunque del corpo, appartengono pure al corpo gli $n+1$ numeri

$$1, \theta, \theta^2, \ldots \theta^{n-1}, \theta^n,$$

fra i quali avrà dunque luogo (essendo il corpo di grado n) una relazione lineare, onde vediamo che: <u>Ogni numero di un corpo algebrico di grado n è radice di un'equazione algebrica a coefficienti interi (che si può supporre irriducibile) ed è di grado n al massimo.</u>

Si può anche dimostrare che fra i numeri di un corpo di grado n ne esistono sempre di quelli (primitivi) il

cui grado è appunto $= n$ (§ 9), e cioè l'equazione irriducibile a cui soddisfano ha appunto il grado n. A noi qui basta dimostrare inversamente come da un numero algebrico θ di grado n viene in effetto generato un corpo K di grado n.

Sia

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = 0$$

l'equazione irriducibile di grado n, a coefficienti razionali interi primi fra loro, a cui θ soddisfa. Nel corpo generato da θ, che indicheremo con $K(\theta)$, qualunque numero α ha la forma

$$\alpha = \frac{A(\theta)}{B(\theta)},$$

con A, B polinomi (a coefficienti razionali o interi) e $B(\theta) \neq 0$. Il polinomio $B(x)$ è primo con $f(x)$, perchè altrimenti (essendo $f(x)$ irriducibile) sarebbe $B(\theta) = 0$. Potremo quindi determinare due polinomi $\varphi(x)$, $\psi(x)$ (§ 8) tali che si abbia

$$\varphi(x) f(x) + \psi(x) B(x) = 1,$$

da cui, ponendo $x = \theta$, risulta

$$\frac{1}{B(\theta)} = \psi(\theta),$$

indi $\alpha = \Phi(\theta)$, essendo Φ un nuovo polinomio in θ. Ma, di-

videndo $\Phi(x)$ per $f(x)$, avremo

$$\Phi(x) = q(x) f(x) + r(x) ,$$

dove il polinomio $r(x)$ è di grado $n-1$ al massimo, e ponendo in questa $x = \theta$ abbiamo

$$\alpha = \Phi(\theta) = r(\theta) .$$

Dunque: Ogni numero α del corpo $K(\theta)$ può porsi sotto la forma

$$(1) \qquad \alpha = r(\theta) = c_0 \theta^{n-1} + c_1 \theta^{n-2} + \dots + c_{n-2} \theta + c_{n-1}$$

coi coefficienti c razionali.

Questa diremo la forma normale del numero α, e dalla irriducibilità di $f(x)$ risulta subito che essa è unica, altrimenti θ soddisferebbe ad un'equazione di grado $< n$.

Se prendiamo ora nel corpo $K(\theta)$ $n+1$ numeri $\omega_0, \omega_1, \dots \omega_n$, che per la (1) avranno la forma

$$\omega_0 = c_{00} \theta^{n-1} + c_{01} \theta^{n-2} + \dots + c_{0,n-1}$$

$$\omega_1 = c_{01} \theta^{n-1} + c_{11} \theta^{n-2} + \dots + c_{1,n-1}$$

$$\dots \dots \dots \dots$$

$$\omega_n = c_{n0} \theta^{n-1} + c_{n1} \theta^{n-2} + \dots + c_{n,n-1}$$

colle c_{ik} razionali, è facile vedere che essi saranno sempre linearmente legati. Poichè infatti, se si considerano nelle n variabili $x_0, x_1, x_2, \dots x_{n-1}$ le $n+1$ forme lineari

$$f_0 = \sum_{r=0}^{r=n-1} c_{0r} x_r \,, \quad f_1 = \sum_{r=0}^{r=n-1} c_{1r} x_r \,, \quad \cdots\cdots \quad f_n = \sum_{r=0}^{r=n-1} c_{nr} x_r \,,$$

si possono certo determinare $n+1$ numeri razionali (anche interi) $\lambda_0, \lambda_1, \cdots \lambda_n$ non tutti nulli, tali che si abbia identicamente

$$\lambda_0 f_0 + \lambda_1 f_1 + \cdots + \lambda_n f_n = 0 \,,$$

e per ciò anche

$$\lambda_0 \omega_0 + \lambda_1 \omega_1 + \cdots + \lambda_n \omega_n = 0 \,, \qquad \text{c. d. d.}$$

D'altronde, l'equazione $f(x)=0$ essendo irriducibile, gli n numeri di $K(\theta)$

$$1, \ \theta, \ \theta^2, \ \ldots \ \theta^{n-1}$$

sono fra loro indipendenti e per ciò: Il corpo $K(\theta)$ generato da un numero algebrico θ di grado n è effettivamente un corpo finito di grado n.

Domandiamo ora: quale è il grado di un qualunque numero α del corpo $K(\theta)$?

Si è già visto sopra che esso è certamente $\leq n$, ed ora andiamo a dimostrare che esso è sempre un divisore di n [in particolare i numeri razionali del corpo sono di grado $=1$].

Poniamo il numero α sotto la forma normale (1)

$$\alpha = r(\theta)$$

e indichiamo con $\theta_1, \theta_2, \ldots \theta_n$ le n radici di $f(x)=0$, cioè i numeri coniugati di θ. Sia $h \leq n$ il grado di α e $\varphi(x)=0$ l'equazione, irriducibile, di grado h a cui α soddisfa. Siccome $\varphi(r(x))=0$ l'equazione $\varphi(r(\theta))=0$ ammette la radice θ dell'equazione irriducibile $f(x)=0$, e però le ammette tutte, cioè

$$\varphi(r(\theta_1))=0, \quad \varphi(r(\theta_2))=0, \ldots \varphi(r(\theta_n))=0.$$

Ora nel polinomio di grado n in x

$$\Phi(x)=(x-r(\theta_1))(x-r(\theta_2))\ldots(x-r(\theta_n))$$

i coefficienti, come funzioni simmetriche di $\theta_1, \theta_2, \ldots \theta_n$, sono numeri razionali. Se gli n numeri

$$(2) \qquad r(\theta_1),\ r(\theta_2) \ldots r(\theta_n)$$

sono tutti distinti, il grado h di $\varphi(x)$ di cui sono tutti radici, non può essere inferiore a n ed è quindi $h=n$. Se poi $h<n$, allora $\Phi(x)$, avendo radici comuni col polinomio irriducibile $\varphi(x)$, lo contiene in fattore e dimostriamo facilmente che $\Phi(x)$ è una potenza esatta di $\varphi(x)$. Sia infatti $(\varphi(x))^q$ la più alta potenza di $\varphi(x)$ che divide $\Phi(x)$, e poniamo

$$\Phi(x)=[\varphi(x)]^q \cdot \psi(x).$$

Se $\psi(x)$ non fosse una costante, esso avrebbe a comune una radice con $\Phi(x)$, indi con $\varphi(x)$ e sarebbe ulteriormen-

te divisibile per $\varphi(x)$. La formula così trovata

$$\Phi(x) = c[\varphi(x)]^q$$

dimostra che si ha $h = \frac{n}{q}$, e gli n numeri (2) sono q a q eguali.

Si osservi che, ponendo $\alpha_i = r(\theta_i)$, i numeri $\alpha_1, \alpha_2 \dots \alpha_n$ sono i coniugati di α, ciascuno ripetuto $\frac{n}{h}$ volte, se h è il grado di α; essi dipendono solo dal corpo K e non dal numero speciale θ col quale si riguarda generato. Nel seguito pei coniugati di un numero α adopreremo anche la notazione: $\alpha, \alpha', \alpha'', \dots \alpha^{(n-1)}$.

§ 12

Norma - Discriminante - Basi del corpo.

Se α è un qualunque numero del corpo, ed $\alpha', \alpha'' \dots \alpha^{(n-1)}$ i suoi coniugati, il loro prodotto si chiama la norma di α e si indica con $N_m(\alpha)$ o $N(\alpha)$:

$$N(\alpha) = \alpha\alpha'\alpha'' \dots \alpha^{(n-1)} = r(\theta_1) r(\theta_2) \cdots r(\theta_n).$$

Egualmente è da considerarsi la somma di tutti questi numeri coniugati, che si chiama la traccia di α, e si indica con

$$T(\alpha) = \alpha + \alpha' + \dots + \alpha^{(n-1)} = r(\theta_1) + r(\theta_2) + \dots + r(\theta_n).$$

Tanto la norma $N(\alpha)$ che la traccia di un numero $T(\alpha)$ sono manifestamente numeri razionali (positivi o negativi); e di più, se α è un intero del corpo, essi sono razionali interi.

Col numero α appartiene anche al corpo il numero $(\alpha-\alpha')(\alpha-\alpha'')\dots(\alpha-\alpha^{(n-1)})$; posto come sopra $\Phi(x)=(x-\alpha)(x-\alpha')\dots(x-\alpha^{(n-1)})$, questo è il valore che assume $\frac{d\Phi(x)}{dx}$ per $x=\alpha$. Hilbert introduce questo numero come la <u>differente</u> di α e lo indica con

$$\delta(\alpha)=(\alpha-\alpha')(\alpha-\alpha'')\cdots(\alpha-\alpha^{(n-1)}).$$

Infine dicesi <u>discriminante</u> $d(\alpha)$ del numero α il quadrato del determinante di Wandermonde

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha & \alpha' & \alpha^{(n-1)} \\ \alpha^2 & \alpha'^2 & (\alpha^{(n-1)})^2 \\ \cdots & \cdots & \cdots \\ \alpha^{(n-1)} & \alpha'^{(n-1)} & (\alpha^{(n-1)})^{n-1} \end{vmatrix} = \Pi(\alpha^{(n)}-\alpha^{(s)})^2,$$

ossia il discriminante di $\Phi(x)$. Manifestamente $d(\alpha)$ è un numero razionale, e, salvo il segno, coincide colla norma della differente $\delta(\alpha)$, precisamente

$$d(\alpha)=(-1)^{\frac{n(n-1)}{2}}N(\delta(\alpha)).$$

Se il numero α è di grado <u>n</u>, la sua differente ed il di-

scriminante sono diversi da zero, e nulli invece in caso contrario.

Consideriamo ora n numeri del corpo $\alpha_1, \alpha_2, \dots \alpha_n$ e indichiamo con $\Delta(\alpha_1, \alpha_2, \dots \alpha_n)$ il quadrato del determinante formato dagli n numeri α e dai loro coniugati

$$\Delta(\alpha_1 \alpha_2 \dots \alpha_n) = \begin{vmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1' & \alpha_2' & \dots & \alpha_n' \\ \dots & \dots & \dots & \dots \\ \alpha_1^{(n-1)} & \alpha_2^{(n-1)} & \dots & \alpha_n^{(n-1)} \end{vmatrix}^2 ;$$

questo dicesi il <u>discriminante</u> degli n numeri $\alpha_1\ \alpha_2 \dots \alpha_n$ ed il suo valore è in ogni caso un numero <u>razionale</u>, anzi un intero se le α sono interi. E infatti, eseguendo il quadrato per colonne risulta un determinante il cui elemento generico è

$$\alpha_i \alpha_k + \alpha_i' \alpha_k' + \dots + \alpha_i^{(n-1)} \alpha_k^{(n-1)} = T(\alpha_i \alpha_k),$$

ed è per ciò un numero razionale. Si osservi che il discriminante degli n numeri $1, \theta, \theta^2, \dots \theta^{n-1}$ è dato da

$$\Delta(1, \theta, \theta^2, \dots \theta^{n-1}) = \prod_{r>s} (\theta_r - \theta_s)^2$$

ed è quindi diverso da zero. [coincide col discriminante dell'equazione che definisce θ, scritta con primo coefficiente $= 1$].

In generale si vede che: <u>Il discriminante di n nu</u>

meri $\Delta(\alpha_1, \alpha_2, \ldots \alpha_n)$ è diverso da zero quando gli n numeri sono linearmente indipendenti ed è nullo quando sono dipendenti. E infatti se scriviamo

$$\alpha_i = \sum_{k=0}^{k=n-1} c_{ik}\, \theta^k \ ,$$

i coefficienti c_{ik} essendo razionali, avremo anche

$$\alpha'_i = \sum_k c_{ik}\, \theta'^k \ , \quad \alpha''_i = \sum_k c_{ik}\, \theta''^k , \ldots\ldots ,$$

onde rilevasi subito

$$\Delta(\alpha_1\, \alpha_2 \ldots \alpha_n) = |c_{ik}|^2 \cdot \Delta(1, \theta, \theta^2, \ldots \theta^{(n-1)})$$

e per ciò $\Delta(\alpha_1, \alpha_2, \ldots \alpha_n)$ è zero soltanto quando è zero il determinante $|c_{ik}|$. Ma, in tal caso, le n forme lineari $f_i = \sum_k c_{ik}\, x_k$ sono linearmente dipendenti, ed esistono quindi n numeri razionali $\lambda_1, \lambda_2, \ldots \lambda_n$ tali che identicamente $\lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_n f_n = 0$, per ciò anche $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n \alpha_n = 0$. Risulta di qui che il segno del discriminante di n numeri del corpo linearmente indipendenti è sempre lo stesso, comunque si scelgano questi numeri.

Ed ora fissiamo la nostra attenzione sui numeri interi del corpo, i quali formano, entro il corpo, un campo d'integrità, riproducendosi per somma, sottrazione e moltiplicazione. È chiaro in primo luogo che possiamo sempre scegliere, entro il corpo n numeri interi indipenden-

ti, poichè se $\alpha_1, \alpha_2, \dots \alpha_n$ sono n numeri indipendenti $[\Delta(\alpha_1, \alpha_2, \dots \alpha_n) \neq 0]$, basta per questo moltiplicare gli n numeri α per un intero razionale r in modo che

$$\omega_1 = r\alpha_1 \;, \; \omega_2 = r\alpha_2 \;, \dots \omega_n = r\alpha_n$$

riescano interi, ciò che è possibile per il teorema b) § 9; allora si ha evidentemente

$$\Delta(\omega_1, \omega_2, \dots \omega_n) = r^{2n} \cdot \Delta(\alpha_1, \alpha_2, \dots \alpha_n) \neq 0$$

e per ciò gli n numeri interi $\omega_1, \omega_2, \dots \omega_n$ sono in effetto indipendenti.

D'ora innanzi intenderemo scelti i sistemi di n numeri indipendenti fra gli interi del corpo, talchè i loro discriminanti $\Delta(\omega_1, \omega_2, \dots \omega_n)$ saranno sempre razionali interi (positivi tutti o tutti negativi). Qualunque altro numero α del corpo, intero o frazionario, si potrà sempre scrivere <u>in uno ed in un sol modo</u> sotto la forma

$$\alpha = h_1\omega_1 + h_2\omega_2 + \dots + h_n\omega_n \,,$$

dove le h_i sono numeri razionali. Se in particolare per le h_i si assumono numeri interi, sarà manifestamente intero anche α; ma può anche darsi che si ottengano dei numeri interi α colle h_i frazionarie. Ora è d'importanza fondamentale per la nostra teoria il dimostrare ko:

Si possono sempre scegliere (ed in infiniti modi) n numeri interi indipendenti $\omega_1, \omega_2, \dots \omega_n$ del corpo, in guisa che nella formula

$$(I) \qquad \alpha = h_1 \omega_1 + h_2 \omega_2 + \dots + h_n \omega_n ,$$

che dà tutti i numeri del corpo percorrendo le h_i i numeri razionali, si ottengano numeri interi α solo quando le h_i assumono valori interi. Un tale sistema $(\omega_1, \omega_2 \dots \omega_n)$ di interi di K si dirà una base del corpo (del campo d'integrità).

Fra gli infiniti sistemi $(\omega_1 \; \omega_2 \dots \omega_n)$ di n interi del corpo indipendenti ve ne saranno certamente di quelli pei quali il valore assoluto $|\Delta(\omega_1 \; \omega_2 \dots \omega_n)|$, del numero razionale intero $\Delta(\omega_1, \omega_2, \dots \omega_n)$ non nullo, raggiunge il suo minimo, ed è facile vedere che se $(\omega_1, \omega_2 \dots \omega_n)$ è un tale sistema, questo forma appunto una base del corpo..

Suppongasi al contrario che si ottenga dalla formula (I) un numero intero α del corpo dando alle h valori razionali non tutti interi, poniamo p.e. che sia h_1 frazionario, scriviamo $h_1 = m + s$ con m intero e s frazione propria $0 < s < 1$. Il numero

$$\overline{\omega}_1 = \alpha - m\omega_1 = s\omega_1 + h_2\omega_2 + \dots + h_n\omega_n$$

è un intero del corpo e pel discriminante $\Delta(\overline{\omega}_1, \omega_2 \dots \omega_n)$ si ha

$$\Delta(\overline{\omega}_1, \omega_2, \dots \omega_n) = \begin{vmatrix} s & h_2 & \dots & h_n \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{vmatrix}^2 \cdot \begin{vmatrix} \omega_1 & \omega_2 & \dots & \omega_n \\ \omega_1' & \omega_2' & \dots & \omega_n' \\ \dots & \dots & \dots & \dots \\ \omega_1^{(n-1)} & \omega_2^{(n-1)} & \dots & \omega_n^{(n-1)} \end{vmatrix}^2$$

cioè

$$\Delta(\overline{\omega}_1, \omega_2 \dots \omega_n) = s^2 \Delta(\omega_1, \omega_2 \dots \omega_n)$$

indi

$$|\Delta(\overline{\omega}_1, \omega_2 \dots \omega_n)| = s^2 |\Delta(\omega_1, \omega_2 \dots \omega_n)| < |\Delta(\omega_1, \omega_2 \dots \omega_n)|,$$

contro l'ipotesi che $|\Delta(\omega_1, \omega_2 \dots \omega_n)|$ avesse già raggiunto il suo minimo.

Dimostrata così l'esistenza di basi del corpo, osserviamo che se $(\omega_1, \omega_2 \dots \omega_n)$ è una tale base ogni altro sistema di n numeri $\alpha_1, \alpha_2 \dots \alpha_n$ (interi o frazionari) del corpo si otterrà con una sostituzione lineare

$$\alpha_i = \sum_{k=1}^{k=n} c_{ik}\omega_k$$

a coefficienti c_{ik} razionali, e sarà $\Delta(\alpha_1, \alpha_2 \dots \alpha_n) = |c_{ik}|^2 (\omega_1, \omega_2 \dots \omega_n)$, onde $\alpha_1, \alpha_2, \dots \alpha_n$ saranno indipendenti allora soltanto che il modulo della sostituzione $C = |c_{ik}|$ sia diverso da zero. In particolare i numeri $\alpha_1, \alpha_2 \dots \alpha_n$.

saranno interi solo quando tutti i coefficienti c_{ik} siano interi (razionali); essi formeranno una nuova base del corpo allora soltanto che il modulo C della sostituzione sia eguale a ± 1. Dunque: Nota una base del corpo $(\omega_1, \omega_2, \dots \omega_n)$, si ottengono tutte le altre assoggettando i numeri della base ad una sostituzione lineare omogenea a coefficienti razionali interi e a determinante $= \pm 1$.

Il numero razionale intero $D = \Delta(\omega_1, \omega_2, \dots \omega_n)$ (positivo o negativo), che è lo stesso per tutte le basi, ha la massima importanza per la costituzione del corpo e dicesi il suo discriminante, od anche il suo numero fondamentale.

§ 13

Unità, numeri associati - Decomponibilità limitata nei corpi finiti.

Riprendiamo ora le considerazioni del § 11 sulla divisibilità degli interi algebrici, sulla loro decomponibilità in fattori, ecc., ma limitandoci agli interi contenuti nel corpo finito K. In primo luogo si osservi che, se α, β sono due numeri interi di K, ed è α divisibile per β nel senso generale (§ 10), il quoziente $\frac{\alpha}{\beta}$, che è un intero algebri-

co, appartiene a K ed è perciò un intero di K. Ne segue che, nel campo d'integrità di K, valgono le leggi elementari della divisibilità, osservate al § 10 pel campo di tutti gli interi algebrici.

Se α è un intero del corpo K, la sua norma $N(\alpha)$ è un intero razionale

$$N(\alpha) = \alpha\, \alpha' \alpha'' \dots \alpha^{(n-1)}$$

manifestamente divisibile per α, sicchè $\frac{N(\alpha)}{\alpha}$ è un altro intero del corpo, l'aggiunto di α secondo Dedekind. Dalla definizione di norma risulta subito il teorema: La norma di un prodotto è uguale al prodotto delle norme dei fattori

$$N(\alpha\beta) = N(\alpha) \cdot N(\beta).$$

Segue di qui subito: Condizione necessaria (non sufficiente) affinchè un intero α di K sia divisibile per un altro intero ρ è che $N(\alpha)$ sia divisibile per $N(\rho)$.

Ogni corpo algebrico finito K contiene in generale, come fra breve dimostreremo, infinite unità ε (§ 11). Siccome una tale unità ε divide 1, così $N(\varepsilon)$ divide $N(1) = 1$, cioè $N(\varepsilon) = \pm 1$; viceversa se $N(\varepsilon) = \pm 1$, il numero ε è una unità perchè dividendo $N(\varepsilon)$, divide 1. Pertanto la ricer-

ca delle unità ε di K equivale alla ricerca dei suoi numeri di norma $= \pm 1$.

Da un numero α del corpo, moltiplicandolo per tutte le unità, si ottengono i suoi infiniti numeri associati che, rispetto alla divisibilità, si comportano come α. Un numero α che non ammetta, in K, altri divisori all'infuori delle unità e dei numeri associati, si riguarderà come <u>indecomponibile</u>; sarà al contrario decomponibile se si può risolvere nel prodotto di due fattori:

$$\alpha = \beta\gamma$$

tali che ciascuno dei fattori β, γ sia diverso da un'unità, cioè $|N(\beta)| > 1$, $|N(\gamma)| > 1$. Allora manifestamente sarà $N(\alpha) = N(\beta) \cdot N(\gamma)$ un numero composto, onde vediamo:

<u>Ogni numero di K la cui norma (in valore assoluto) sia un numero primo ordinario è indecomponibile in K.</u>

Supponiamo ora al contrario α decomponibile in K e sia

$$\alpha = \beta_1 \cdot \beta_2 \ldots \beta_s$$

una sua decomposizione <u>essenziale</u> in s fattori, con che intendiamo dire che nessuno degli s numeri β sia un'unità. Siccome

$$N(\alpha) = N(\beta_1)\, N(\beta_2) \ldots N(\beta_s)$$

e ciascuno dei fattori a destra (in valore assoluto) è ≥ 2, è chiaro che il numero s sarà necessariamente limitato. Siccome poi la decomposizione dell'intero razionale $N(\alpha)$ non può farsi che in un numero finito di modi, e d'altronde due numeri le cui norme abbiano egual valore assoluto sono associati, se si riguardano come non essenzialmente distinte due decomposizioni di α quando ciascun fattore dell'una trovi il suo associato in un fattore dell'altra, è chiaro che si può concludere:

- Ogni numero decomponibile in K può rappresentarsi soltanto in un numero finito di modi essenzialmente distinti quale prodotto di fattori indecomponibili.

A differenza dunque di quanto accadeva nel corpo di tutti i numeri algebrici (§ 11), ove la decomponibilità era illimitata, qui invece, nei corpi finiti K, si ha sempre decomponibilità limitata. Ma basta già l'esempio particolare addotto al § 7 pel corpo quadratico di base $(1, i\sqrt{5})$ per intendere che nei corpi superiori si presenta generalmente il fenomeno della decomponibilità, limi-

tata bensì, ma non unica, e i numeri indecomponibili non funzionano più come numeri primi. Come già abbiamo detto al § 7, si riesce a ristabilire le leggi dell'aritmetica ordinaria colla teoria degli ideali, di cui ci occuperemo nel Capitolo seguente.

§ 14

Esempio dei corpi quadratici.

Prima di procedere oltre nella teoria generale, sarà opportuno illustrare le nozioni fondamentali stabilite in un esempio più semplice, quello dei corpi di 2° grado o quadratici. Possiamo partire da un'equazione di 2° grado (irriducibile) con primo coefficiente = 1 e gli altri due interi

$$\theta^2 + b\theta + c = 0,$$

che definisce l'irrazionalità (quadratica) fondamentale

$$\theta = \frac{-b + \sqrt{b^2 - 4c}}{2},$$

ove naturalmente si dovrà supporre che il numero $b^2 - 4c$ non sia un quadrato perfetto. Indicando con β^2 il massimo fattore quadrato di $b^2 - 4c$, poniamo

$$b^2 - 4c = \beta^2 d$$

con d (positivo o negativo) privo di fattori quadrati. Fissia-mo p.e. di scegliere per $\sqrt{d}$ il valore positivo se $d > 0$, o quel-lo col coefficiente dell'immaginario positivo se $d < 0$, e scri-viamo

$$\theta = \frac{-b+\beta\sqrt{d}}{2}.$$

Ogni numero (intero o frazionario) del corpo ha la forma

$$\alpha = \frac{p+q\sqrt{d}}{r}$$

con p, q, r interi, senza divisore comune. Il coniugato di α è $\alpha' = \frac{p-q\sqrt{d}}{r}$ e perchè α sia intero occorre che tali siano la traccia $T(\alpha) = \frac{2p}{r}$ e la norma $N(\alpha) = \frac{p^2-dq^2}{r^2}$; ma an-che viceversa se sono interi $T(\alpha)$ e $N(\alpha)$, tale è anche α, avendosi

$$\alpha^2 - \alpha T(\alpha) + N(\alpha) = 0.$$

Dobbiamo dunque cercare come devesi prendere la ter-na di numeri interi (p, q, r) privi di divisore comune, affinchè i due numeri

$$T = \frac{2p}{r}, \qquad S = \frac{p^2-dq^2}{r^2}$$

siano interi. Se supponiamo dapprima r dispari, dovrà r dividere p e quindi essere primo con q; ma allora $\frac{p^2}{r^2} - S = \frac{dq^2}{r^2}$ dovendo essere intero, sarà d divisibile per r^2. E siccome d non ha fattori quadrati, sarà necessaria

mente $r=1$ e gli interi α corrispondenti in K avranno semplicemente la forma

$$\alpha = p + q\sqrt{d}\ .$$

Sia in secondo luogo r pari, poniamo $r = 2r'$ con r' divisore di p $p = r'p'$ indi primo con q.

Essendo intero $S = \frac{p'^2 r'^2 - d q^2}{4 r'^2}$, sarà anche intero $\frac{d q^2}{r'^2} = p'^2 - 4S$, indi come sopra $r' = 1$. In questo caso deve essere dunque $r = 2$ e i numeri p, q <u>non tutti due pari</u> tali che sia

$$(1) \qquad p^2 - dq^2 \equiv 0 \pmod 4 ;$$

e siccome <u>d</u> non è divisibile per 4 (che è un quadrato) non potranno nemmeno p, q essere l'uno pari l'altro dispari, e saranno per conseguenza tutti due dispari, ciò che è compatibile colla (1) solo quando $d \equiv 1 \pmod 4$. In conclusione i numeri interi del corpo quadratico $K(\sqrt{d})$ sono soltanto quelli della forma: $p + q\sqrt{d}$ (p, q interi), se $d \equiv 2, 3 \pmod 4$, ai quali, nel caso $d \equiv 1 \pmod 4$ occorre aggiungere gli altri

$$\frac{p + q\sqrt{d}}{2}, \quad \text{con} \quad p \equiv q \equiv 1 \pmod 2 .$$

Di qui si vede che per avere una base (ω_1, ω_2) del corpo quadratico conviene fare

$$\omega_1 = 1 \qquad \omega_2 = \sqrt{d}, \quad \text{nei casi } d \equiv 2, 3 \pmod 4$$

$$\omega_1 = 1 \quad \omega_2 = \frac{1+\sqrt{d}}{2}, \quad \text{nel caso } d \equiv 1 \pmod 4.$$

Corrispondentemente pel numero fondamentale D del corpo (discriminante) abbiamo

$$D = \Delta(\omega_1, \omega_2) = \begin{vmatrix} 1, & \sqrt{d} \\ 1, & -\sqrt{d} \end{vmatrix}^2 = 4d, \text{ se } d \equiv 2, 3 \pmod 4$$

$$D = \Delta(\omega_1, \omega_2) = \begin{vmatrix} 1, & \frac{1+\sqrt{d}}{2} \\ 1, & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d, \quad \text{se } d \equiv 1 \pmod 4)$$

Si possono del resto compendiare tutti i casi assumendo per base

$$\omega_1 = 1, \quad \omega_2 = \frac{D+\sqrt{D}}{2};$$

così ogni numero intero del corpo avrà la forma

$$(2) \qquad \frac{x+y\sqrt{D}}{2}, \quad \text{però con } x \equiv Dy \pmod 2.$$

In particolare si osservi che se $d=-1$, il numero fondamentale è $D=-4$ ed abbiamo il corpo quadratico di Gauss; se $d=-3$ anche $D=-3$ ed il corpo è quello di Jacobi-Eisenstein della radice cubica ε dell'unità.

La norma di un intero

$$\alpha = \frac{x+y\sqrt{D}}{2} \quad (x \equiv Dy \pmod 2))$$

del corpo è

$$N(\alpha) = \frac{x^2 - Dy^2}{4},$$

e la ricerca delle unità ($N\alpha = \pm 1$) equivale alla riso-

luzione in interi x, y dell'equazione detta di Pell-
-Fermat

$$(a) \qquad x^2 - Dy^2 = \pm 4,$$

la quale però nel caso di D pari $= 4d$ richiede che x sia pari $= 2t$, e ponendo $y = u$ risulta l'equazione

$$(b) \qquad t^2 - du^2 = \pm 1.$$

Distinguiamo ora i due casi di D negativo, ovvero positivo. Nel primo caso il corpo è immaginario (contiene anche numeri immaginarii) e dei due segni nella (a) entra in considerazione solo quello superiore. Di più appena $|D| > 4$, l'equazione di Pell non ha altre soluzioni che $x = \pm 2$, $y = 0$ ed esistono le due sole unità ± 1. Fanno eccezione i due casi $D = -4$, $D = -3$, nel primo dei quali si hanno le quattro unità: ± 1, $\pm i$ (campo di Gauss), e nel secondo le sei unità: ± 1, $\pm \varepsilon$, $\pm \varepsilon^2$ (campo di Jacobi). Sempre però, si osservi: le unità di un corpo quadratico immaginario sono radici m^{me} dell'unità ($m = 2, 4, 6$).

Se D è positivo, l'equazione (a) di Pell è sempre solubile, almeno pel segno superiore, con numeri x, y interi diversi da zero, in infiniti modi ed esistono quindi innumerevoli unità di norma $= +1$, eventualmente an-

che di quelle con norma = −1. Queste circostanze sono ben note nell'aritmetica elementare delle forme binarie quadratiche, ma non sono che casi particolarissimi della teoria generale delle unità nei corpi algebrici le cui leggi furono scoperte da Dirichlet.

Alla esposizione della ricerca delle unità, secondo Dirichlet, premettiamo la dimostrazione di alcuni notevoli teoremi sui sistemi di forme lineari, dovuti a Minkowski, che sono fondamentali per molte ricerche della teoria dei numeri. Questi teoremi hanno anche una notevolissima interpretazione geometrica, ed appunto per questa via furono scoperti dall'autore (Minkowski - Geometrie der Zahlen [Teubner, 1910]) più elementarmente nelle: Diophantische Approximationen [Teubner, 1910]). Noi qui seguiremo, per brevità, la via aritmetica algebrica molto semplice per la quale vennero stabiliti da Hurwitz.

§ 15

Sistemi di forme lineari a coefficienti interi. – Numero delle classi.

Consideriamo nel presente paragrafo soltanto forme lineari in n variabili $x_1, x_2, \dots x_n$, con coefficienti razionali interi. Siano $f_1, f_2, \dots f_n$ n tali forme

$$(1) \qquad f_i = \sum_{k=1}^{k=n} a_{ik} x_k \qquad (i = 1, 2, \dots n),$$

che supponiamo indipendenti, il cui determinante $D = |a_{ik}|$ sarà dunque razionale intero non nullo e, senza alterare la generalità, si potrà supporre $D > 0$. Si dirà che un'altra forma F (a coefficienti interi) è congrua a zero, rispetto ai moduli $f_1, f_2, \dots f_n$, e si scrive

$$F \equiv 0 \pmod{f_1, f_2, \cdots f_n},$$

quando F sia un aggregato lineare, a coefficienti interi, di $f_1, f_2, \cdots f_n$. Similmente due forme F, Φ si diranno congrue fra loro, in simboli $F \equiv \Phi \pmod{f_1, f_2, \cdots f_n}$ quando $F - \Phi \equiv 0 \pmod{f_1, f_2, \cdots f_n}$. È visibile che per le congruenze così definite valgono le solite leggi elementari, onde le forme si distribuiranno in classi ponendo in una medesima classe quelle che sono congrue con una fissa, indi fra loro. Risolvendo le (1) rapporto alle x_i, al-

biamo

$$(2) \qquad x_\lambda = \frac{1}{D} \sum_i A_{i\lambda} f_i \, ,$$

essendo $A_{i\lambda}$ il complemento algebrico di $a_{i\lambda}$ in D. È chiaro che se $D = 1$, tutte le x_λ sono congrue a zero (modd $f_1, f_2, \cdots f_n$), e per ciò anche qualunque altra forma, onde in questo caso tutte le forme costituiscono una sola classe. In generale dimostriamo:

Il numero delle classi di forme è sempre finito ed uguale a D, cioè esistono D forme incongrue fra loro (modd f_1, $f_2, \cdots f_n$) ed ogni altra forma è congrua con una di queste.

Consideriamo le prime m variabili $x_1, x_2, \dots x_m$ $(1 \le m \le n)$; siccome in ogni caso per le (2) si ha $D x_m \equiv 0$ (modd $f_1, f_2, \dots f_n$), esisterà un minimo numero intero positivo, che indicheremo con $c_{m,m}$, tale che sussista una congruenza della forma

$$c_{m1} x_1 + c_{m2} x_2 + \cdots + c_{mm} x_m \equiv 0 \quad (\text{modd } f_1, f_2, \cdots f_n),$$

quando gli altri interi $c_{m1}, c_{m2}, \dots c_{mm}$ siano scelti in modo conveniente. Poniamo allora

$$\varphi_m = c_{m1} x_1 + c_{m2} x_2 + \cdots + c_{mm} x_m \, ,$$

e consideriamo le n forme $\varphi_1, \varphi_2, \dots \varphi_n$, che sono tutte $\equiv 0$

(modd $f_1, f_2, \cdots f_n$) ed hanno il determinante

$$\frac{\partial(\varphi_1, \varphi_2, \cdots \varphi_n)}{\partial(x_1, x_2, \cdots x_n)} = c_{11}\, c_{22}, \cdots c_{nn}\,;$$

dimostreremo che le forme

$$(3) \qquad \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n\,,$$

nelle quali in generale λ_i percorra i c_{ii} valori $0, 1, 2 \cdots c_{ii}-1$, sono tutte incongrue fra loro (modd $f_1, f_2, \cdots f_n$), e qualunque altra forma F è congrua con una di queste.

Con ciò sarà provato che il numero h delle classi è finito, ed è

$$h = c_{11}\, c_{22} \cdots c_{nn}\,,$$

dopo di che dovremo successivamente provare che è $h = D$.

Che due forme del tipo (3) siano incongrue fra loro si dimostra subito osservando che se si avesse

$$\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n \equiv \lambda'_1 x_1 + \lambda'_2 x_2 + \cdots + \lambda'_n x_n \pmod{f_1, f_2 \cdots f_n},$$

indi

$$(\lambda_1 - \lambda'_1) x_1 + (\lambda_2 - \lambda'_2) x_2 + \cdots + (\lambda_n - \lambda'_n) x_n \equiv 0,$$

siccome $(\lambda_n - \lambda'_n) < c_{nn}$ ne consegue subito, pel significato di c_{nn}, $\lambda_n - \lambda'_n = 0$ o $\lambda_n = \lambda'_n$. Ma allora rimane

$$(\lambda_1 - \lambda'_1) x_1 + (\lambda_1 - \lambda'_2) x_2 + \cdots + (\lambda_{n-1} - \lambda'_{n-1}) x_{n-1} \equiv 0,$$

da cui deducesi nel medesimo modo $\lambda_{n-1} = \lambda'_{n-1}$; e così via.

In secondo luogo proviamo ora che qualunque forma

F è congrua con una delle (3). Sia

$$F = h_1 x_1 + h_2 x_2 + \cdots + h_n x_n \quad \text{(colle } h_i \text{ intere)}$$

e dividendo h_n per c_{nn} poniamo

$$h_n = q_n c_{nn} + \lambda_n \qquad 0 \leq \lambda_n < c_{nn}.$$

La forma $F - q_n \varphi_n = F - q_n (c_{n1} x_1 + c_{n2} x_2 + \cdots + c_{nn} x_n) = \sum_{i=1}^{i=n-1} h'_i x_i + \lambda_n x_n$ è congrua con F (perchè $\varphi_n \equiv 0$) e il coefficiente λ_n di x_n è non negativo e inferiore a c_{nn}. Proseguiamo dividendo

$$h'_{n-1} = h_{n-1} - q_n c_{n,n-1}$$

per $c_{n-1,n-1}$ e ponendo $h'_{n-1} = q_{n-1} c_{n-1,n-1} + \lambda_{n-1}$, con $0 \leq \lambda_{n-1} < c_{n-1,n-1}$, sottraggiamo ancora da $F - q_n \varphi_n$ il prodotto $q_{n-1} \varphi_{n-1}$. Così abbiamo una nuova forma $\equiv F$, e cioè

$$F - q_n \varphi_n - q_{n-1} \varphi_{n-1} = \sum_{i=1}^{i=n-2} h''_i x_i + \lambda_{n-1} x_{n-1} + \lambda_n x_n;$$

e continuando nello stesso modo troveremo da ultimo

$$F - q_n \varphi_n - q_{n-1} \varphi_{n-1} \cdots - q_1 \varphi_1 = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$$

cioè una forma $\equiv F$ del tipo (3).

Dimostriamo infine che si ha: $c_{11} c_{22} \cdots c_{nn} = D$, considerando che le n forme $\varphi_1, \varphi_2, \cdots \varphi_n$, come congrue a zero, sono tutte combinazioni lineari a coefficienti interi di $f_1, f_2, \cdots f_n$; ma anche viceversa qualunque f_k, essendo $\equiv 0$, col sottrarvi una combinazione lineare di $\varphi_1, \varphi_2, \cdots \varphi_n$ si riduce, per quanto precede al tipo (3), ma con tutti i coefficienti $\lambda_i = 0$,

ossia le $f_1, f_2, \cdots f_n$ sono a loro volta combinazioni lineari a coefficienti interi di $\varphi_1, \varphi_2, \cdots \varphi_n$. Ma siccome le une e le altre forme sono indipendenti, le due sostituzioni lineari colle quali si passa dalle f alle φ, e viceversa dalle φ alle f si compongono nell'identità, e per ciò i loro determinanti sono $= \pm 1$. E allora avendosi

$$\frac{\partial(f_1, f_2, \cdots f_n)}{\partial(x_1, x_2, \cdots x_n)} = \mathfrak{D}, \quad \frac{\partial(f_1, f_2, \cdots f_n)}{\partial(\varphi_1, \varphi_2, \cdots \varphi_n)} = \pm 1, \quad \frac{\partial(\varphi_1, \varphi_2, \cdots \varphi_n)}{\partial(x_1, x_2, \cdots x_n)} = c_{11}\, c_{22} \cdots c_{nn},$$

moltiplicando le due ultime risulta appunto

$$\mathfrak{D} = c_{11}\, c_{22} \cdots c_{nn} \qquad \text{c.d.d.}$$

Immaginiamo ora che, nelle n forme lineari (1): $f_1, f_2, \cdots f_n$ a coefficienti interi a_{ik} e determinante $\mathfrak{D} > 0$, si facciano assumere alle variabili x_i tutti i sistemi di valori interi, con esclusione di $(0, 0, \dots 0)$; le n forme f_i assumeranno ogni volta valori interi non tutti nulli, e come primo e più semplice caso dei risultati di Minkowski possiamo stabilire un minimo per questi sistemi di valori col teorema: Si possono dare alle x_i valori interi (non tutti nulli) tali che ciascun numero f_i non superi in valore assoluto $\sqrt[n]{\mathfrak{D}}$.

Consideriamo, in n variabili $\xi_1, \xi_2, \cdots \xi_n$ le n forme lineari

$$(4) \qquad \psi_i = \sum_{k=1}^{k=n} a_{ki}\, \xi_k \,,$$

che corrispondono alla sostituzione trasposta di quella che figura nelle (1) per le forme f_i. Il determinante delle ψ è eguale ancora a D e fra le combinazioni lineari a coefficienti interi delle ξ.

$$(a) \qquad c_1\xi_1 + c_2\xi_2 + \cdots + c_n\xi_n$$

il numero delle incongrue (modd $\psi_1, \psi_2, \dots \psi_n$) è appunto $= D$, pel teorema precedente.

Sia ora r il massimo intero contenuto in $\sqrt[n]{D}$, talchè

$$r^n \leq D < (r+1)^n,$$

e diamo nella (a), a ciascuna delle c, gli $r+1$ valori

$$c_i = 0, 1, 2, \dots r.$$

Così abbiamo $(r+1)^n > D$ forme due delle quali almeno sono congrue (modd $\psi_1, \psi_2, \dots \psi_n$), e nella loro differenza

$$\lambda_1\xi_1 + \lambda_2\xi_2 + \cdots + \lambda_n\xi_n = \sum_{i=1}^{i=n} \lambda_i\xi_i$$

abbiamo una forma non identicamente nulla i cui coefficienti λ_i non superano $\sqrt[n]{D}$ e che risulta una combinazione lineare intera a coefficienti interi μ_i delle ψ_i scriviamo

$$\sum_{i=1}^{i=n} \lambda_i\xi_i = \sum_{i=1}^{i=n} \mu_i\psi_i \,,$$

e cioè per le (4)

$$\sum_{i=1}^{i=n} \lambda_i \xi_i = \sum_{i,k} a_{ki} \gamma_i \xi_k = \sum_i \left(\sum_k a_{ik} \gamma_k \right) \xi_i$$

ed abbiamo quindi identificando

$$\lambda_i = \sum_{k=1}^{k=n} a_{ik} \gamma_k . \qquad (i = 1, 2, \ldots n)$$

Se dunque nelle $\underline{n}$ forme (1) diamo alle x_k i valori interi γ_k, che non sono tutti nulli (perchè non sono nulli tutti i λ_i), la f_i acquista il valore di λ_i e si ha quindi in valore assoluto

$$|f_i| \leq \sqrt[n]{D} , \quad \text{c. d. d.}$$

§ 16

I teoremi di Minkowski per le forme lineari a coefficienti reali o complessi.

Togliamo ora la condizione che i coefficienti a_{ik} delle $\underline{n}$ forme f_i siano interi, e supponiamo dapprima soltanto che siano reali, ed abbiamo determinante $D > 0$; proviamo che sussiste sempre la proprietà di minimo data dal:

I) Teorema di Minkowski Se le n forme lineari

$$f_i = \sum_{k=1}^{k=n} a_{ik} x_k$$

hanno coefficienti reali, e determinante $D = |a_{ik}|$ positivo, si possono sempre dare alle variabili x valori in-

teri, non tutti nulli, tali che i valori assunti dalle forme f_i soddisfino alle diseguaglianze

$$|f_i| \leq \sqrt[n]{D}.$$

Dividiamo la dimostrazione in due parti, supponendo prima che i coefficienti a_{ik} siano numeri razionali, e considerando poi il caso generale

a) i coefficienti a_{ik} siano razionali. Indichiamo con N il minimo multiplo comune di tutti i loro denominatori, talchè i numeri Na_{ik} sono tutti razionali interi. Nelle n forme a coefficienti interi

$$F_i = Nf_i = \sum_k Na_{ik} x_k ,$$

col determinante $\Delta = N^n D$, si possono dare alle x valori interi, non tutti nulli, tali che risulti

$$|F_i| \leq \sqrt[n]{\Delta} \leq N \sqrt[n]{D} ,$$

e corrispondentemente si hanno per le f_i le limitazioni richieste

$$|f_i| = \frac{1}{N} |F_i| \leq \sqrt[n]{D} , \quad \text{c. d. d.}$$

b) i coefficienti a_{ik} siano reali qualunque. Possiamo approssimare ciascun numero a_{ik} con una successione di numeri razionali

$$a_{ik}^{(1)} , \ a_{ik}^{(2)} , \ a_{ik}^{(3)} , \dots$$

per modo che sia

$$a_{ik} = \lim_{r=\infty} a_{ik}^{(r)} \,,$$

e le $\underline{n}$ forme f_i verranno così approssimate dalla successione di forme a coefficienti razionali

$$f_i^{(r)} = \sum_k a_{ik}^{(r)} x_k \qquad r = 1, 2, \dots \infty$$

Indicando con $\mathcal{D}^{(r)}$ il determinante delle $f_1^{(r)}, f_2^{(r)} \dots f_n^{(r)}$ sarà

$$\lim_{r=\infty} \mathcal{D}^{(r)} = \mathcal{D} \,,$$

sicchè da un certo valore di $\underline{r}$ in poi sarà p.e.

$$(b) \qquad \mathcal{D}^{(r)} > \frac{\mathcal{D}}{2} \,.$$

Senz'altro, sopprimendo la serie finita di approssimazioni precedenti, possiamo supporre questa disuguaglianza verificata per tutti i valori di $r = 1, 2, 3, \dots$ Per ogni valore fissato di r si può, per quanto abbiamo dimostrato in a), dare alle x_k valori interi $x_k^{(r)}$ non tutti nulli, tali che risulti pei valori

$$(c) \qquad y_i^{(r)} = \sum_k a_{ik}^{(r)} x_k^{(r)}$$

la limitazione

$$|y_i^{(r)}| \leq \sqrt[n]{\mathcal{D}^{(r)}} \,.$$

Siccome $\lim_{r=\infty} \mathcal{D}^{(r)} = \mathcal{D}$, risulta di qui che le $y_i^{(r)}$ restano limitate uniformemente e così pure le $a_{ik}^{(r)}$ a causa di

$\lim_{r=\infty} a_{ik}^{(r)} = a_{ik}$. Se indichiamo con A una quantità positiva sufficientemente grande, avremo dunque per tutti i valori di $i, k = 1, 2, \dots n$, $r = 1, 2, 3, \dots$

$$|a_{ik}^{(r)}| < A\ , \quad |y_i^{(r)}| < A\ .$$

Se ora risolviamo le equazioni (c) rispetto alle $x_k^{(r)}$, otteniamo ciascuna di queste come quoziente di due determinanti d'ordine n, il determinante denominatore essendo $D^{(r)} > \frac{D}{2}$, mentre quello al numeratore ha ogni elemento in valore assoluto $< A$, e perciò è certamente in valore assoluto $< n! A^n$ [o servendosi del noto teorema di Hadamard sul massimo di un determinante $< n^{\frac{n}{2}} A^n$]; ne risulta per tutti i valori di n la limitazione fissa

$$|x_k^{(r)}| < \frac{n! A^n}{\frac{D}{2}} \quad \left(o < \frac{n^{\frac{n}{2}} A^n}{\frac{D}{2}} \text{ col teorema di Hadamard}\right)$$

Tutti i numeri interi della successione infinita

$$x_1^{(r)},\ x_2^{(r)} \dots x_n^{(r)} \qquad (r = 1, 2, 3 \dots \infty)$$

essendo così limitati, esisterà almeno un sistema di tali numeri interi $x_1, x_2, \dots x_n$ che sarà ripetuto infinite volte, diciamo per $r = r_1, r_2, r_3 \dots \infty$, ed allora tutte le corrispondenti

$$y_i^{(r_s)} = \sum_k a_{ik}^{(r_s)} x_k \qquad \text{per } s = 1, 2, \dots \infty,$$

soddisfano alle diseguaglianze

$$\left| y_i^{(s)} \right| \leq \sqrt[n]{\mathcal{D}^{(s)}}.$$

Ma poichè $y_i = \sum_k a_{ik} x_k$ si ha

$$\lim_{s=\infty} y_i^{(s)} = y_i \quad , \quad \lim_{s=\infty} \mathcal{D}^{(s)} = \mathcal{D},$$

e pei numeri interi trovati x_k risulteranno dunque verificate le diseguaglianze

$$\left| \sum_{k=1}^{k=n} a_{ik} x_k \right| \leq \sqrt[n]{\mathcal{D}} \;, \qquad \text{c. d. d.}$$

Come corollario del teorema I) di Minkowski si ha anche il seguente:

<u>Teorema II)</u>. <u>Sotto le stesse condizioni del teorema I), scelte n qualità positive $\mathcal{D}_1, \mathcal{D}_2, \dots \mathcal{D}_n$ tali che sia $\mathcal{D}_1 \mathcal{D}_2 \dots \mathcal{D}_n = \mathcal{D}$, si possono dare alle x valori interi, non tutti nulli, tali che i valori assunti dalle forme f_i verifichino le diseguaglianze</u>

$$|f_i| \leq \mathcal{D}_i \qquad (i = 1, 2, \dots n).$$

Per dimostrare questo basta applicare il teorema stesso I) alle nuove forme $\frac{f_i}{\mathcal{D}_i}$, il cui determinante è $= 1$.

Passiamo ora a considerare il caso di $\underline{n}$ forme lineari indipendenti $f_1, f_2, \dots f_n$ a coefficienti complessi, colla condizione però che nel sistema, insieme ad ogni forma f a coefficienti complessi, figuri la sua <u>comples-</u>

sa coniugata $\bar{f}$. Intanto il determinante D di queste forme, certamente diverso da zero, cangiando i in $-i$, resterà lo stesso o cangierà di segno secondo che il numero s delle coppie di forme complesse coniugate sarà pari o dispari e sarà quindi D reale se s è pari, D puramente immaginario per s dispari. Ordiniamo le n forme f_i nel sistema facendo precedere quelli reali, diciamo in numero di r, seguite dalle s coppie complesse coniugate, rappresentato nello schema

$$f_1\,,\ f_2\,,\cdots f_r\,,\ (\varphi_1,\bar{\varphi}_1)\,,\ (\varphi_2,\bar{\varphi}_2)\cdots(\varphi_s,\bar{\varphi}_s) \qquad r+2s=n$$

Consideriamo allora le n forme, tutte reali

$$F_1=f_1\,,\ F_2=f_2\,,\ \dots F_r=f_r\,,\ F_{r+1}=\frac{\varphi_1+\bar{\varphi}_1}{\sqrt{2}}\,,\ F_{r+2}=\frac{\varphi_1-\bar{\varphi}_1}{i\sqrt{2}}\,,\ F_{r+3}=\frac{\varphi_2+\bar{\varphi}_2}{\sqrt{2}}\,,$$

$$F_{r+4}=\frac{\varphi_2+\bar{\varphi}_2}{i\sqrt{2}}\,,\ F_{n-1}=\frac{\varphi_s+\bar{\varphi}_s}{\sqrt{2}}\,,\ F_n=\frac{\varphi_s-\bar{\varphi}_s}{i\sqrt{2}}$$

dedotte dalle f con una sostituzione lineare il cui modulo si calcola subito nel determinante d'ordine 21

$$\begin{vmatrix} \frac{1}{\sqrt{2}}\,, & \frac{1}{\sqrt{2}}\,, & 0 & 0 & \dots & 0 & 0 \\ \frac{1}{i\sqrt{2}}\,, & -\frac{1}{i\sqrt{2}}\,, & 0 & 0 & & & \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & & 0 & 0 \\ 0 & 0 & \frac{1}{i\sqrt{2}} & -\frac{1}{i\sqrt{2}} & & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & 0 & 0 & & \frac{1}{i\sqrt{2}} & -\frac{1}{i\sqrt{2}} \end{vmatrix} = i^s$$

onde, indicando con Δ il determinante (reale) di $F_1, F_2 \dots F_n$, sarà

$$\Delta = i^s \mathcal{D} \quad \text{(conformemente all'osservazione superiore } \bar{\mathcal{D}} = (-1)^s \mathcal{D}\text{)}$$

A queste forme reali F_i applichiamo il teorema II), scegliendo n quantità positive $\mathcal{D}_1, \mathcal{D}_2, \dots \mathcal{D}_n$ tali che sia $\mathcal{D}_1 \mathcal{D}_2 \dots \dots \mathcal{D}_n = |\Delta| = |\mathcal{D}|$, le prime r delle quali siano coordinate alle forme $f_1, f_2, \dots f_n$ e le seguenti, a coppie eguali, alle s coppie complesse coniugate $(\varphi_\rho, \bar{\varphi}_\rho)$ $\rho = 1, 2, \dots s$. Pel teorema II), si potranno scegliere n valori interi non tutti nulli per le x, per modo che risulti

$$|F_i| \leq \mathcal{D}_i \qquad (i = 1, 2, \dots n).$$

Allora avremo

$$|f_1| \leq \mathcal{D}_1, \quad |f_2| \leq \mathcal{D}_2, \dots \dots |f_r| \leq \mathcal{D}_r,$$

e da

$$\begin{cases} \varphi_1 \sqrt{2} = F_{r+1} + i F_{r+2} \\ \bar{\varphi}_1 \sqrt{2} = F_{r+1} - i F_{r+2} \end{cases}$$

avendosi

$$|F_{r+1}| \leq \mathcal{D}_{r+1} \qquad |F_{r+2}| \leq \mathcal{D}_{r+2} = \mathcal{D}_{r+1}$$

risulta

$$|\varphi_1| \sqrt{2} = \sqrt{F_{r+1}^2 + F_{r+2}^2} \leq \sqrt{2}\, \mathcal{D}_{r+1}, \quad o \quad |\varphi_1| \leq \mathcal{D}_{r+1}.$$

Abbiamo così stabilito il nuovo teorema:

III) Date n forme lineari in $x_1, x_2, \dots x_n$ di cui r reali, e le rimanenti $n-r = 2s$ a coppie complesse coniugate, con determinante $D \neq 0$, scelgansi n quantità reali positive $D_1, D_2, \dots D_n$ coordinate alle forme, così che a due forme complesse coniugate corrispondano due D_k eguali, e tali che sia $D_1 D_2 \dots D_n = |D|$. Si possono allora dare alle variabili x_i valori interi, non tutti nulli, tali che i moduli dei valori assunti dalle forme f_i soddisfino alle diseguaglianze

$$|f_i| \leq D_i \qquad (i = 1, 2, \dots n).$$

Si osservi che per tal modo risulta anche soddisfatta la diseguaglianza

$$|f_1 f_2 \cdots f_n| \leq |D|,$$

cioè: esistono valori interi non tutti nulli delle x che rendono il modulo del prodotto delle n forme lineari non superiore al modulo del determinante.

§ 17

Applicazione al numero fondamentale D del corpo.

Una prima applicazione di questi teoremi sulle forme lineari ha fatto il Minkowski stesso alla dimostrazione di un fatto di fondamentale importanza per la

teoria dei corpi algebrici e cioè che:

A) Il discriminante D o numero fondamentale (§ 12) di un corpo algebrico (non razionale) è in ogni caso diverso da ± 1. - Ne segue che questo numero fondamentale possiede almeno un fattore primo p. I fattori primi di D diconsi anche i numeri primi critici del corpo; il loro ufficio è assimilabile, per l'aritmetica generale dei corpi algebrici, a quello dei punti di diramazione per le funzioni algebriche di una variabile (Minkowski).

Alla dimostrazione del teorema A) premettiamo alcune considerazioni sui corpi coniugati di un dato corpo $K(\theta)$, cioè sugli n corpi generati dalle n radici della equazione fondamentale irriducibile di grado n a cui θ soddisfa. Ciascuna di queste radici, che indicheremo nel seguito con

$$\theta = \theta^{(1)}, \theta^{(2)}, \dots \theta^{(n)},$$

è un numero algebrico di grado n; esse generano gli n corpi coniugati

$$K^{(1)}, K^{(2)}, \dots K^{(n)}$$

Questi n corpi non sono sempre essenzialmente distinti ma possono in parte coincidere sino a formare un

unico corpo, che allora dicesi un corpo normale, od anche un corpo di Galois. La considerazione di questi corpi di Galois è importantissima perchè appunto la teoria di Galois delle equazioni algebriche riconduce essenzialmente l'aritmetica dei corpi algebrici a quella dei corpi normali (V. § 39).

Ritornando al caso generale, osserviamo che fra i numeri di due qualunque dei corpi coniugati, siano $K^{(r)}$, $K^{(s)}$, risulta stabilita una corrispondenza biunivoca, tale che ad ogni numero $\alpha^{(r)}$ del primo, posto sotto la forma normale (§ 11)

$$\alpha^{(r)} = \varphi(\theta^{(r)}),$$

dove φ è un polinomio di grado $\leq n-1$ con coefficienti razionali, corrisponde nel secondo $K^{(s)}$ il numero coniugato

$$\alpha^{(s)} = \varphi(\theta^{(s)}).$$

Proprietà essenziale di questa corrispondenza è che: ogni relazione razionale fra più numeri dell'un corpo si traduce nella medesima relazione fra i numeri corrispondenti dell'altro, ciò che è una conseguenza della irriducibilità dell'equazione fondamentale. [Se un po-

linomio $F(x)$ si annulla per $x=\theta$ si annulla anche per tutti i numeri coniugati di θ]. In particolare si osservi: a qualunque numero razionale di $K^{(1)}$ corrisponde lo stesso numero razionale in $K^{(2)}$.

Ciò premesso, prendiamo una base di $K^{(1)}$, e sia formata dagli $\underline{n}$ numeri interi

$$\omega_1^{(1)},\ \omega_2^{(1)} \dots \omega_n^{(1)},$$

sicchè ogni intero di $K^{(1)}$ sarà dato da

$$\alpha^{(1)} = h_1\,\omega_1^{(1)} + h_2\,\omega_2^{(1)} + \dots + h_n\,\omega_n^{(1)},$$

dove $h_1, h_2, \dots h_n$ percorrono tutti gli interi razionali. Per quanto si è detto sopra, formeranno una base di $K^{(r)}$ gli $\underline{n}$ numeri $\omega_1^{(r)}, \omega_2^{(r)}, \dots \omega_n^{(r)}$, il numero $\alpha^{(r)}$ di $K^{(r)}$ corrispondente ad $\alpha^{(1)}$ di $K^{(1)}$ essendo dato da

$$\alpha^{(r)} = h_1\,\omega_1^{(r)} + h_2\,\omega_2^{(r)} + \dots + h_n\,\omega_n^{(r)} \qquad (r = 1, 2, \dots n).$$

A causa della variabilità delle $\underline{h}$, questo ci conduce ad associare a ciascuno dei corpi coniugati $K^{(i)}$ una forma lineare corrispondente sia

$$(1) \qquad f_i = \omega_1^{(i)} x_1 + \omega_2^{(i)} x_2 + \dots + \omega_n^{(i)} x_n \qquad (i = 1, 2, \dots n).$$

Venendo ora alla dimostrazione del teorema A), escluderemo senz'altro, oltre il caso del corpo razionale $n=1$, quello dei corpi quadratici trattato al § 14 perchè qui-

vi abbiamo già constatato che in tal caso è sempre certamente $|D| > 1$ e il teorema A) è allora verificato. L'equazione fondamentale $f(x) = 0$, che definisce θ, abbia r radici reali s coppie di radici complesse coniugate, talchè $r + 2s = n$, ed avremo $r + s > 1$ perchè $r + s = 1$ si ha unicamente nel caso escluso del corpo razionale $r = 1$, $s = 0$, $n = 1$, e nell'altro $r = 0$, $s = 1$, $n = 2$ del corpo quadratico (immaginario) egualmente escluso. Ordiniamo gli n corpi coniugati così che i primi r: $K^{(1)}, K^{(2)}, \dots K^{(r)}$ siano reali, ed i seguenti $2s$ immaginarii a coppie di complessi coniugati, sicchè le forme lineari (1) associate a questi corpi risulteranno ordinate al modo del § precedente.
Il quadrato del determinante di queste forme

$$\begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \dots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \dots & \omega_n^{(2)} \\ \dots & \dots & \dots & \dots \\ \omega_1^{(n)} & \omega_2^{(n)} & \dots & \omega_n^{(n)} \end{vmatrix}$$

coincide precisamente con $\Delta(\omega_1, \omega_2, \cdots \omega_n)$ cioè (§ 12) col numero fondamentale D del corpo, e per ciò il modulo del determinante stesso è $= \sqrt{(D)}$.

Applicando allora il teorema III) (§ 12) di Minkowski,

prendiamo $r+s$ quantità positive $c_1, c_2, \cdots c_r, c_{r+1} \cdots c_{r+s}$,
tali che si abbia

$$(2) \qquad c_1 c_2 \cdots c_r c_{r+1}^2 c_{r+2}^2 \cdots c_{r+s}^2 = \sqrt{|\mathfrak{D}|}$$

e del resto arbitrarie, sicchè ponendo poi

$$\mathfrak{D}_1 = c_1 \;,\; \mathfrak{D}_2 = c_2 \;, \cdots \mathfrak{D}_r = c_r \;,\; \mathfrak{D}_{r+1} = \mathfrak{D}_{r+2} = c_{r+1} \cdots \mathfrak{D}_{r+2s-1} = \mathfrak{D}_{r+2s} = c_{r+s},$$

saranno appunto soddisfatte le condizioni del teorema III).
Potremo due dare alle variabili x nelle forme f_i valori interi non tutti nulli così da soddisfare alle diseguaglianze

$$(3) \qquad |f_i| \leq \mathfrak{D}_i \qquad (i = 1, 2, \cdots n)$$

$$(4) \qquad |f_1 f_2 \cdots f_n| \leq \sqrt{|\mathfrak{D}|} .$$

I valori che così assumono le forme f_i sono quelli di n interi coniugati diversi da zero

$$\alpha^{(1)}, \alpha^{(2)}, \cdots \alpha^{(n)},$$

e l'ultima diseguaglianza dimostra che si ha

$$(5) \qquad |\alpha^{(1)} \alpha^{(2)} \cdots \alpha^{(n)}| = |N(\alpha)| \leq \sqrt{|\mathfrak{D}|} .$$

Ora $|N(\alpha)|$ è un intero razionale positivo, e quindi se vale in questa (5) il segno < si ha anche $|\mathfrak{D}| > 1$ come si voleva. Resta solo la possibilità $|\mathfrak{D}| = 1$ con $|N(\alpha)| = 1$ nel qual caso però avremo per le (3)

$$\frac{|\alpha^{(i)}|}{\mathfrak{D}_i} \leq 1 \;,\; \frac{|\alpha^{(1)}|}{\mathfrak{D}_1} \cdot \frac{|\alpha^{(2)}|}{\mathfrak{D}_2} \cdots \frac{|\alpha^{(n)}|}{\mathfrak{D}_n} = 1 ,$$

onde ciascuna delle n quantità positive $\frac{|\alpha^{(i)}|}{D_i}$ sarebbe $=1$. In tal caso D_i, come modulo di un intero algebrico, sarebbe un intero algebrico [perchè il complesso coniugato di un intero algebrico è anche intero, per ciò anche il loro prodotto e la sua radice quadrata (§ 10); ma siccome per ipotesi $r+s>1$, possiamo sempre scegliere ad arbitrio $r+s-1$ dei numeri c, p.e. possiamo fare c_1 eguale a un numero razionale non intero, e la detta possibilità resta allora esclusa. Come si vede, questa dimostrazione del teorema A) include anche il caso dei corpi quadratici reali ($r=2$, $s=0$), dove del resto abbiamo già visto direttamente che $|D|>1$.

§ 18

Dimostrazione di Hilbert.

Lo stesso teorema A) si può dimostrare con un procedimento alquanto variato, dovuto ad Hilbert, che ci condurrà anche a stabilire un altro importante teorema.

Cominciamo dalla dimostrazione di un lemma, utile anche per altre ricerche:

a) Esiste soltanto un numero finito di numeri interi algebrici, di grado dato n, tali che il loro modulo, e insieme quelli di tutti i loro coniugati, non superino un dato limite A.

Sia infatti

$$f(x) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_{n-1} x + c_n = 0$$

l'equazione di grado n, con primo coefficiente $= 1$ e gli altri interi (razionali), colle radici $\theta^{(1)}, \theta^{(2)}, \dots \theta^{(n)}$ (numeri coniugati) e supponiamo $|\theta^{(i)}| < A$ $(i = 1, 2, \dots n)$.

Dalle formole elementari

$$-c_1 = \sum \theta^{(i)}, \quad c_2 = \sum \theta^{(i)}\theta^{(k)}, \quad -c_3 = \sum \theta^{(i)}\theta^{(k)}\theta^{(l)}, \dots$$

risulta subito

$$|c_1| \leq \sum |\theta^{(i)}|, \quad |c_2| \leq \sum |\theta^{(i)}||\theta^{(k)}| \dots$$

Per ciò gli interi $c_1, c_2, \dots$ risultano limitati in valore assoluto e non possono quindi assumere che un numero finito di valori.

Ora riprendendo, coi teoremi di Minkowski, la dimostrazione del teorema A) stabiliamo quest'altro lemma:

b) Nel corpo $K(\vartheta)$ di numero fondamentale D esiste almeno un intero α, diverso da zero, tale che per il numero stesso $\alpha^{(1)}$ e pei suoi coniugati sussistano le disuguaglianze

$$(1)\qquad |\alpha^{(1)}| \leqq \sqrt{|\mathfrak{D}|}\ ,\quad |\alpha^{(2)}|<1\ ,|\alpha^{(3)}|<1 \cdots |\alpha^{(n)}|<1$$

(di modulo $\leq \sqrt{|\mathfrak{D}|}$ e coi moduli dei coniugati tutti <1).

Cominciamo dal dimostrare che esistono sempre dei numeri α (interi) soddisfacenti alle diseguaglianze

$$(2)\qquad |\alpha^{(1)}|<\sqrt{|\mathfrak{D}|}+1\ ,\quad |\alpha^{(2)}|<1,\quad |\alpha^{(3)}|<1, \cdots |\alpha^{(n)}|<1$$

Per questo prendiamo un numero positivo σ, abbastanza piccolo, pel quale sia soddisfatta la diseguaglianza

$$(\alpha)\qquad (1+\sigma)^{n-1}\sqrt{|\mathfrak{D}|} < \sqrt{|\mathfrak{D}|}+1 \quad \left(\text{ossia } 0<\sigma<\left(\frac{1}{\sqrt{|\mathfrak{D}|}}+1\right)^{\frac{1}{n-1}}-1\right)$$

e pei numeri $D_1\ D_2 \ldots D_n$ del § 17 assumiamo

$$(3)\qquad D_1 = (1+\sigma)^{n-1}\sqrt{|\mathfrak{D}|}\ ,\quad D_2 = D_3 = \cdots = D_n = \frac{1}{1+\sigma}\ ,$$

colla qual cosa soddisfacciamo alla condizione

$$D_1\, D_2 \ldots D_n = \sqrt{|\mathfrak{D}|}\ .$$

Dal teorema III) di Minkowski risulta che esistono interi α soddisfacenti alle diseguaglianze

$$(4)\qquad |\alpha^{(1)}| \leq (1+\sigma)^{n-1}\sqrt{|\mathfrak{D}|}\ ,\quad |\alpha^{(2)}| \leq \frac{1}{1+\sigma} \cdots |\alpha^{(n)}| \leq \frac{1}{1+\sigma}\ ,$$

e per ciò anche, a causa della (α), alle diseguaglianze (2).

Ora questi numeri α effettivamente esistenti, che soddisfano le (2) sono pel lemma a) in numero finito, e fra questi ve ne sarà uno $\underline{\alpha}$ pel quale $|\alpha^{(1)}|$ avrà

il minimo valore possibile, che indichiamo con φ. Basterà dimostrare che questo minimo φ di $|\alpha^{(1)}|$ è necessariamente $\leq \sqrt{|D|}$. Se supponiamo al contrario $\sqrt{|D|} < \varphi$, basterà prendere una costante σ positiva abbastanza piccola per soddisfare alla diseguaglianza

$$|1+\sigma|^{n-1}\sqrt{|D|} < \varphi$$

e prendere ancora $D_1\ D_2 \dots D_n$ dalle (3). Ne risulterà l'esistenza di un altro numero ω soddisfacente alle (4) e però alle

$$|\omega^{(1)}| < \varphi\ ,\ |\omega^{(2)}| < 1\ , \cdots |\omega^{(n)}| < 1,$$

indi, poichè $\varphi < \sqrt{|D|}+1$, alle (2), in contraddizione col significato di φ come minimo.

Dal lemma b) così stabilito segue subito nuovamente il teorema A) § 17, ove si faccia il prodotto delle diseguaglianze (1), ciò che dà

$$|N(\alpha)| < \sqrt{|D|},$$

e per ciò, essendo $|N(\alpha)| \geq 1$, risulta $|D| > 1$.

Da questo nuovo procedimento per la dimostrazione del teorema A) possiamo trarre di più un altra importante conseguenza contenuta nel seguente teorema (Hermite - Minkowski):

B) Fra i corpi algebrici di grado n non ne esiste che un numero finito aventi un assegnato numero fondamentale D.

In ogni tale corpo K esiste infatti qualche intero α che soddisfa alle diseguaglianze (1), e vediamo facilmente che un tale intero α è di grado n, cioè genera il corpo K. Per ciò basta provare, secondo il § 11, che $\alpha^{(1)}$ è diverso da tutti i coniugati $\alpha^{(2)}, \alpha^{(3)} \dots \alpha^{(n)}$, e questo risulta da che $\alpha^{(2)}, \alpha^{(3)}, \dots \alpha^{(n)}$ hanno ciascuno modulo < 1 e quindi $\alpha^{(1)}$ modulo > 1 perchè $|N(\alpha)| = |\alpha^{(1)}| \cdot |\alpha^{(2)}| \cdots |\alpha^{(n)}| \geq 1$. Ora pel lemma a), essendo assegnato D, non vi ha che un numero finito di tali interi algebrici α, e questo prova il teorema B). Ricerche ulteriori di Minkowski, colle quali si trova un limite inferiore pel valore assoluto del numero fondamentale D di un corpo di dato grado, assicurano ancora più che: esiste solo un numero finito di corpi collo stesso numero fondamentale D.

§ 19

Preliminari alla ricerca di Dirichlet delle unità del corpo.

Le importanti questioni che riguardano l'esistenza

delle unità nei corpi algebrici, e le leggi che le governano, vennero risolute da Dirichlet con un geniale procedimento, che generalizza a tutti i corpi algebrici quello tenuto da Lagrange per l'equazione di Pell, cioè per le unità nei corpi quadratici reali § 14.

Il metodo di Dirichlet si fonda sopra un lemma, per sè notevole, che assicura l'esistenza, in ogni corpo $K(\theta)$, di numeri interi che, insieme ai coniugati, soddisfano coi loro moduli a determinate disuguaglianze.

Consideriamo, come al § 17, gli n corpi coniugati

$$K^{(1)}, K^{(2)}, \dots K^{(n)},$$

dei quali i primi r siano i reali ed i seguenti $2s$ immaginarii susseguentisi a coppie di complessi coniugati. Si ha $r+2s=n$, mentre: il numero

$$\nu = r+s$$

ha il significato più importante per le unità del corpo. Noi supporremo senz'altro $\nu>1$, perchè $\nu=1$ si ha soltanto, come già si è avvertito al § 17, nei casi del corpo razionale e dei corpi quadratici immaginarii, ove la ricerca delle unità è immediata. Fissate, co-

me al § 17, le basi

$$\left[\omega_1^{(i)},\ \omega_2^{(i)} \dots \omega_n^{(i)}\right] \qquad (i = 1, 2, \dots n)$$

per questi corpi coniugati, consideriamo $\underline{n}$ loro interi generici corrispondenti (coniugati)

$$(1) \quad \begin{cases} \xi^{(1)} = h_1\,\omega_1^{(1)} + h_2\,\omega_2^{(1)} + \dots + h_n\,\omega_n^{(1)} \\ \xi^{(2)} = h_1\,\omega_1^{(2)} + h_2\,\omega_2^{(2)} + \dots + h_n\,\omega_n^{(2)} \\ \dots\dots\dots\dots\dots\dots\dots \\ \xi^{(n)} = h_1\,\omega_1^{(n)} + h_2\,\omega_2^{(n)} + \dots + h_n\,\omega_n^{(n)} \end{cases}$$

dove le h_i percorrono tutti gli interi razionali. Essendo ora $\underline{k}$ un numero razionale intero positivo arbitrario, diamo nelle (1) alle h_i valori che non superino k in valore assoluto, e pel modulo di ciascuno dei numeri $\xi^{(i)}$, così ottenuti, varrà la limitazione

$$\left|\xi^{(i)}\right| \leq k\left\{\left|\omega_1^{(i)}\right| + \left|\omega_2^{(i)}\right| + \dots + \left|\omega_n^{(i)}\right|\right\}.$$

Le basi $\left[\omega_1^{(r)}, \omega_2^{(r)}, \dots \omega_n^{(r)}\right]$ essendo fissate una volta per tutte, se indichiamo con $\underline{c}$ la più grande delle $\underline{n}$ somme

$$\left|\omega_1^{(i)}\right| + \left|\omega_2^{(i)}\right| + \dots + \left|\omega_n^{(i)}\right| \qquad (i = 1, 2, \dots n)$$

varrà dunque per tutti i nostri numeri ξ la limitazione

$$(2) \qquad \left|\xi^{(i)}\right| \leq ck \qquad (i = 1, 2, \dots n).$$

Ripartiamo ora gli n corpi in due gruppi, che diciamo A e B, in modo affatto arbitrario, purchè siano soddisfatte le condizioni seguenti: 1) due corpi complessi coniugati prendano posto in un medesimo gruppo, 2) ciascun gruppo contenga almeno un corpo, condizioni queste che possono sempre soddisfarsi, essendo per ipotesi $\nu > 1$. Per un qualunque intero ξ del corpo, noi indicheremo col simbolo α quei coniugati di ξ che appartengono al gruppo A, e con β quelli che appartengono all'altro B, e stabiliremo il lemma seguente:

C) Data una costante positiva a, comunque piccola, ed un'altra b (positiva) comunque grande, esiste sempre nel corpo $K(\vartheta)$ un intero ξ la cui norma è inferiore in valore assoluto a $(3c)^n$, e tale che i suoi coniugati α appartenenti al gruppo A soddisfino alla diseguaglianza $|\alpha| < a$, e quelli β del gruppo B all'altra $|\beta| > b$.

Nel gruppo A è contenuto un certo numero $t \geq 1$ di corpi, e per ogni intero ξ altrettanti interi α (coniugati di ξ)

$$\alpha_1, \alpha_2, \cdots, \alpha_t,$$

alcuni dei quali saranno reali, altri a coppie com-

plessi coniugati. Scindendo ciascun $\underline{\alpha}$ complesso nella sua parte reale ed immaginaria $\alpha = \alpha' + i\,\alpha''$, lo surrogheremo colle due parti componenti (α', α'') e i $\underline{t}$ valori reali così risultanti indicheremo con

$$(3) \qquad w_1\ ,\ w_2\ , \dots w_t\ .$$

Fissiamo il numero razionale intero positivo k per ora ad arbitrio, ed attribuiamo nelle formole (1) alle <u>coordinate</u> h_i del numero ξ i valori

$$h_i = 0, 1, 2, \dots k-1\ , k\ .$$

Ne risulteranno $(k+1)^n$ numeri differenti ξ, tutti soddisfacenti alla diseguaglianza (2), e in particolare pei corrispondenti α del gruppo A sarà

$$|\alpha| \leq ck\ .$$

Pel significato delle quantità reali $\underline{w}$ della serie (3), ciascuno di questi $\underline{t}$ valori delle $\underline{w}$ giacerà dunque nell'intervallo $(-ck, +ck)$. Suddividiamo allora questo intervallo, d'ampiezza $2ck$, in intervalli parziali eguali, fondandoci sulle osservazioni seguenti.

Siccome $n > t \geq 1$ e $k > 0$, vale la diseguaglianza

$$(k+1)^{\frac{n}{t}} - k^{\frac{n}{t}} > 1\ ,$$

come si rileva semplicemente osservando che, per x po-

sitivo e per $s>1$, la funzione $f(x)=(x+1)^s-x^s-1$, nulla per $x=0$, è crescente nell'intervallo $(0, +\infty)$ perchè ivi $f(x)>0$. Ne segue che, nell'interno dell'intervallo $(k^{\frac{n}{t}}$, $(k+1)^{\frac{n}{t}})$ di ampiezza >1, esiste almeno un numero intero m razionale positivo, che soddisfa dunque alle condizioni

$$(4) \qquad k^{\frac{n}{t}} < m < (k+1)^{\frac{n}{t}}, \quad \text{o} \quad k^n < m^t < (k+1)^n.$$

Dividiamo allora il detto intervallo $(-ck, ck)$ in m intervalli parziali eguali, la cui ampiezza δ, sarà

$$(5) \qquad \delta = \frac{2ck}{m} < \frac{2c}{k^{\frac{n}{t}-1}} .$$

Ogni quantità reale σ nell'intervallo $(-ck, ck)$ cadrà in uno di questi m intervalli e, per non lasciare alcuna ambiguità, noi diremo che σ appartiene all'intervallo i^{mo} quando sia $-ck+(i-1)\delta \leq \sigma < -ck+i\delta$, e il numero intero i si dirà per un momento l'indice della quantità reale σ. Alle t quantità reali (3) compete così una determinata successione di indici

$$(6) \qquad r_1, r_2 \dots r_t ,$$

ciascuno dei quali è un numero della serie $1, 2, \dots m$. Le successioni (6) differenti possibili sono dunque m^t; mentre i numeri ξ differenti, a ciascun dei quali

compete una di quelle successioni, sono in numero di $(k+1)^n$, che per la (4) è $> m$. Se ne conclude che: a due diversi dei nostri numeri ξ competerà la medesima successione (6) di indici, cioè le w corrispondenti per questi due numeri ξ cadranno nel medesimo intervallo e le rispettive differenze $w_i - \bar{w}_i$ non supereranno δ in valore assoluto. Dopo ciò se consideriamo la differenza η di quei due numeri ξ, questo è un intero non nullo del corpo, le cui coordinate sono tutte (in valore assoluto) $\leq k$, e per quanto precede, indicando con $w_i' = w_i - \bar{w}_i$ i valori delle quantità w_i appartenenti al numero η, si ha $|w_i'| \leq \delta$. Per ogni numero α coniugato di η, ed appartenente al gruppo A, le due parti reale ed immaginaria non superino δ e si ha quindi certamente

$$|\alpha| \leq \delta\sqrt{2},$$

cioè per la (5)

$$|\alpha| < \frac{2\sqrt{2}\,c}{k^{\frac{n}{2}-1}},$$

e a più forte ragione

$$(7) \qquad |\alpha| < \frac{3c}{k^{\frac{n}{2}-1}}.$$

A questo punto già una parte del lemma C) risulta

dimostrata, poichè, per quanto piccola sia la quantità positiva data $\underline{a}$, possiamo prendere il numero intero (razionale) k così grande che risulti

$$\frac{3c}{k^{\frac{n}{t}-1}} < a\,,$$

ed allora, pel numero intero η di $K(\theta)$ sopra trovato, i corrispondenti α del gruppo A soddisferanno alle condizioni $|\alpha| < a$.

Prendendo ora in considerazione gli altri numeri β, coniugati di η, e appartenenti al gruppo B, indichiamo per brevità con $P = \Pi\alpha$ il prodotto di tutti i $\underline{t}$ numeri α e con $Q = \Pi\beta$ il prodotto dei rimanenti $n-t$ numeri β, onde avremo

$$N(\eta) = PQ\,, \quad |N(\eta)| = |P|\cdot|Q|$$

Siccome i $\underline{t}$ moduli dei numeri α soddisfano alla (7), il loro prodotto $|P|$ soddisfa all'altra

$$(8) \qquad |P| < \frac{(3c)^t}{k^{n-t}}\,.$$

D'altra parte ciascuno degli $n-t$ numeri β soddisfa alla (2) (come gli α)

$$|\beta| \leq ck$$

e per ciò

$$|Q| < (ck)^{n-t}\,,$$

e quindi $|P|\,|Q| < 3^t c^n$. Dunque a più forte ragione $|P|\,|Q| < (3c)^n$, cioè

$$|N(\eta)| < (3c)^n,$$

come è asserito nell'enunciato del lemma C). In fine, se consideriamo che $N(\eta)$ è razionale intero non nullo, e perciò $|P|\,|Q| \geq 1$, ne viene

$$|Q| \geq \frac{1}{|P|},$$

e siccome dalla (7) $\frac{1}{|P|} > (3c)^{-t} k^{n-t}$, a fortiori

$$(9) \qquad |Q| > (3c)^{-t} k^{n-t}.$$

Se dal prodotto Q si isola un qualunque numero β, e si considera che gli $n-t-1$ fattori rimanenti hanno ciascuno un modulo $\leq ck$, risulta

$$|Q| \leq |\beta|\,(ck)^{n-t-1}$$

e quindi

$$|\beta| \geq \frac{|Q|}{(ck)^{n-t-1}},$$

onde anche per la (9)

$$(10) \qquad |\beta| \geq \frac{k}{3^t c^{n-1}}$$

Considerando in fine quest'ultima diseguaglianza, insieme alla (7), è chiaro che, per quanto piccola sia la quantità positiva $\underline{a}$, e per quanto grande l'altra $\underline{b}$, si può prendere l'intero k tanto grande da rendere ad un tempo

$$\frac{3c}{k^{\frac{n}{t}-1}} < a, \qquad \frac{k}{3^t c^{n-1}} > b$$

e tutte le condizioni del lemma enunciato saranno così soddisfatte.

Come semplice conseguenza del teorema così dimostrato, si osservi che in ogni corpo algebrico $K(\theta)$, appena il numero sopra indicato con ν sia > 1, esistono interi non nulli di modulo piccolo a piacere, ciò che possiamo significare così: Escluso il corpo dei numeri razionali, ed esclusi i corpi quadratici immaginari, ogni altro corpo algebrico $K(\theta)$ contiene numeri interi infinitesimi. Così anche, rappresentando i numeri interi di $K(\theta)$ nel consueto modo sul piano complesso, in ogni intorno di un intero, esistono infiniti altri interi, ossia nel gruppo G di punti immagini degli interi di $K(\theta)$ ogni punto di G appartiene al gruppo derivato [secondo le denominazioni della teoria degli aggregati il gruppo G è concentrato]

§ 20

Esistenza delle unità - Le $\nu-1$ unità indipendenti.

Applicando ripetutamente il lemma C), è facile ora

costruire una catena infinita di numeri interi del corpo

$$(11) \qquad \eta_1, \eta_2, \eta_3 \ldots\ldots,$$

per ciascuno dei quali il valore assoluto della norma $N(\eta)$ sia $< (3c)^n$, e tali che, mantenendo la divisione dei corpi $K^{(i)}$ nei due gruppi A e B, i moduli dei coniugati di un numero η della catena appartenenti al gruppo A siano minori di tutti gli analoghi per i numeri η precedenti, e invece quelli appartenenti al gruppo B maggiori di tutti gli analoghi per gli η precedenti nella catena.

Si scelga per ciò, ad arbitrio il primo η_1 nella catena (11) (purchè soddisfi alla condizione $(N(\eta_1) < (3c)^n)$ e si indichi con a_1 il più piccolo, con b_1 il più grande dei moduli dei coniugati appartenenti rispettivamente ai gruppi A e B. Prendasi ora, secondo il lemma C), un secondo numero η_2, con $|N(\eta_2)| < (3c)^n$, i cui coniugati α appartenenti ad A abbiano moduli tutti $< a_1$ e quelli β appartenenti moduli $> b_1$. Così, detto a_2 il più piccolo dei primi e b_2 il più grande dei secondi, sarà

$$a_2 < a_1 \quad , \quad b_2 > b_1 \; ;$$

e nello stesso modo si prosegua per la costruzione de-

gli infiniti numeri η della catena (11). Le norme di questi numeri

$$(11^*) \qquad N(\eta_1), N(\eta_2), N(\eta_3), \dots$$

sono tutti razionali interi inferiori in valore assoluto a $(3c)^n$, e per ciò una almeno di queste norme si troverà nella serie (11*) ripetuta <u>infinite volte</u>. Diciamo

$$(12) \qquad \xi_1, \xi_2, \xi_3, \dots$$

questa serie infinita di numeri appartenenti alla serie (11), ed aventi la stessa norma $N(\xi) = q$. Le corrispondenti coordinate h_i di questi numeri ξ nella rappresentazione (1) § 17

$$\xi = h_1 \omega_1 + h_2 \omega_2 + \cdots h_n \omega_n$$

possono ricevere, ciascuna, rispetto al modulo q, solo q valori incongrui, e per ciò la combinazione $[h_1, h_2, \dots h_n]$ solo $|q|^n$ valori diversi. Pertanto, nella serie (12), accadrà infinite volte che due numeri diversi ξ abbiano le loro rispettive coordinate h congrue fra loro (mod q); siano λ, μ due tali numeri con

$$N(\lambda) = N(\mu) = q.$$

La differenza $\lambda - \mu$ è un intero di $K(\theta)$, diverso da zero, e con coordinate $\equiv 0 \pmod q$; onde segue

$$\lambda - \mu = q \cdot \Omega$$

con Ω intero nel corpo. Siccome $\frac{N(\lambda)}{\lambda}$, $\frac{N(\mu)}{\mu}$, cioè $\frac{q}{\lambda}$, $\frac{q}{\mu}$, sono due numeri interi in $K(\theta)$ (§ 13), ne segue che $\frac{\lambda}{\mu}$, $\frac{\mu}{\lambda}$ sono ambedue interi e per ciò: il numero $\frac{\lambda}{\mu}$ è un'unità ε del corpo. Se, nella serie (12) delle ξ, il numero λ precede il numero μ, i moduli dei numeri coniugati di λ, appartenenti al gruppo A, sono tutti maggiori dei corrispondenti per μ nello stesso gruppo, e perciò in questo gruppo A i moduli dei coniugati di ε sono tutti > 1; al contrario quelli del gruppo B tutti < 1. Siamo giunti pertanto al seguente risultato fondamentale:

α) Esiste nel corpo $K(\theta)$ un'unità ε, di norma $N(\varepsilon) = +1$, tale che i moduli dei numeri coniugati di ε nel gruppo A sono > 1, e quelli nel gruppo $B < 1$.

È chiaro che tutte le potenze di ε con esponenti interi, positivi o negativi, sono altrettante unità, tutte diverse fra loro, vale a dire questa ε non è una radice dell'unità (nel senso ordinario).

Per studiare ora la legge di distribuzione di tutte le unità contenute in $K(\theta)$, ci conviene introdurre la seguente nozione di logaritmi coniugati di un'unità

ε. Gli n corpi coniugati $K^{(1)}, K^{(2)} \dots K^{(n)}$ sono distribuiti in r corpi reali, e in $\underline{s}$ coppie di corpi complessi coniugati, per modo che $r+s=\nu$. In ciascuna delle $\underline{s}$ coppie serbiamo soltanto uno dei corpi, tralasciando l'altro, sicchè restano ν corpi, diciamo

$$(a) \qquad K^{(1)}, K^{(2)} \dots K^{(\nu)},$$

dei quali r reali e i rimanenti $\nu - r$ complessi, per modo che non vi è contenuta alcuna coppia di complessi coniugati, ma questi ν corpi, insieme ai complessi coniugati dei $\nu - r$ immaginarii, dànno tutti gli $\underline{n}$ corpi. Allora se ε è un' unità ed $\varepsilon^{(q)}$ il numero coniugato di ε, appartenente al corpo $K^{(q)}$, noi porremo

$$(13) \quad \begin{cases} l_q(\varepsilon) = \log |\varepsilon^{(q)}| & \text{se il corpo } K^{(q)} \text{ è reale} \\ l_q(\varepsilon) = 2\log |\varepsilon^{(q)}| & \text{se } K^{(q)} \text{ è immaginario,} \end{cases}$$

cioè $l_q(\varepsilon)$ rappresenterà, nel primo caso, la parte reale del logaritmo neperiano di $|\varepsilon^{(q)}|$, nel secondo il suo doppio. Dando a $\underline{q}$ i suoi ν valori, avremo così ν di questi numeri (reali)

$$l_1(\varepsilon), \; l_2(\varepsilon), \dots l_\nu(\varepsilon),$$

che si diranno i ν logaritmi coniugati dell' unità ε e saranno positivi o negativi secondo che $|\varepsilon^{(q)}| > 1$ ovve-

ro $|\varepsilon^{(q)}|<1$. In ogni caso, siccome $|N(\varepsilon)|=1$, il prodotto dei moduli di tutti i coniugati di ε è $=1$, onde per la definizione stessa di $l_q(\varepsilon)$ risulta:

I ν logaritmi coniugati di un'unità ε sono sempre legati dalla relazione

$$(14) \qquad l_1(\varepsilon)+l_2(\varepsilon)+\cdots+l_\nu(\varepsilon)=0.$$

Colla nozione di logaritmi coniugati, il risultato sopra ottenuto per l'esistenza di un'unità ε di $N(\varepsilon)=+1$ assume la forma seguente:

α') Se i ν corpi (a) si distribuiscono ad arbitrio in due gruppi A e B (per modo che ciascuno dei due gruppi contenga almeno un corpo), esiste in $K(\theta)$ un'unità ε, di norma positiva, i cui logaritmi coniugati del gruppo A sono positivi, quelli del gruppo B negativi.

Siano ora

$$\varepsilon_1,\ \varepsilon_2,\ \ldots\ \varepsilon_\nu$$

ν unità del corpo e poniamo per brevità $l_i(\varepsilon^{(q)})=l_{iq}$ $(i,q=1,2,\ldots n)$; risulta dalla (14)

$$\begin{gathered}
l_{11}+l_{21}+\cdots+l_{\nu 1}=0\\
l_{12}+l_{22}+\cdots+l_{\nu 2}=0\\
\cdots\cdots\cdots\cdots\\
l_{1\nu}+l_{2\nu}+\cdots+l_{\nu\nu}=0,
\end{gathered}$$

e per ciò il determinante

$$\begin{vmatrix} l_{11} & l_{21} & \dots & l_{\nu 1} \\ l_{12} & l_{22} & \dots & l_{\nu 2} \\ \dots & \dots & \dots & \dots \\ l_{1\nu} & l_{2\nu} & \dots & l_{\nu\nu} \end{vmatrix}$$

è certamente nullo. Ora è d'importanza fondamentale per il seguito dimostrare il teorema:

β) Si possono sempre trovare nel corpo $K(\theta)$ $\nu-1$ unità $\varepsilon_1, \varepsilon_2, \cdots \varepsilon_{\nu-1}$, di norma positiva $N(\varepsilon) = +1$, tali che ponendo $l_{iq} = l_i(\varepsilon^{(q)})$ per $i, q = 1, 2, \dots n-1$ il determinante

$$\mathcal{L}(\varepsilon_1, \varepsilon_2, \dots \varepsilon_{\nu-1}) = \begin{vmatrix} l_{11} & l_{12} & \dots & l_{1,\nu-1} \\ l_{21} & l_{22} & \dots & l_{2,\nu-1} \\ \dots & \dots & \dots & \dots \\ l_{\nu-1,1} & l_{\nu-1,2} & \dots & l_{\nu-1,\nu-1} \end{vmatrix}$$

riesca positivo.

Intanto, se $\nu = 2$, questo teorema risulta come caso particolare dal teorema α'), perchè, attribuendo allora $K^{(1)}$ ad A e $K^{(2)}$ a B, esiste un'unità ε con $l_1(\varepsilon) > 0$.

Sia ora $\nu > 2$, e denotando con m un numero razionale intero, compreso fra 1 e ν

$$1 < m < \nu,$$

supponiamo già trovate $m-1$ unità $\varepsilon_1, \varepsilon_2, \dots \varepsilon_{m-1}$ tali che sia

$$(15) \qquad \begin{vmatrix} l_{11} & l_{12} & \dots & l_{1,m-1} \\ l_{21} & l_{22} & \dots & l_{2,m-1} \\ \dots & \dots & \dots & \dots \\ l_{m-1,1} & l_{m-1,2} & \dots & l_{m-1,m-1} \end{vmatrix} > 0 ;$$

dimostriamo col teorema α') che se ne può aggiungere una m^{ma}, tale che sia

$$\mathcal{L} = \begin{vmatrix} l_{11} & l_{12} & \dots & l_{1,m} \\ l_{21} & l_{22} & \dots & l_{2m} \\ \dots & \dots & \dots & \dots \\ l_{m1} & l_{m2} & \dots & l_{mm} \end{vmatrix} > 0 .$$

Cominciando allora da $m = 2$, si potrà giungere fino a $m = \nu - 1$ e resterà stabilito il teorema β). Sviluppando il determinante $\mathcal{L}$ per gli elementi dell'ultima colonna, scriviamo

$$(16) \qquad \mathcal{L} = \Lambda_1 l_{1m} + \Lambda_2 l_{2m} + \dots + \Lambda_m l_{mm} ;$$

dove Λ_m sarà precisamente il determinante (15) per ipotesi positivo; invece gli altri $\Lambda_1, \Lambda_2, \dots \Lambda_{m-1}$ formati coi logaritmi di $\varepsilon_1, \varepsilon_2, \dots \varepsilon_{m-1}$ possono essere positivi, negativi o nulli. Ripartiamo i $\nu > m$ corpi

$$K^{(1)}, K^{(2)} \dots K^{(m)} K^{(m+1)} \dots K^{(\nu)},$$

attribuendo al primo gruppo A il corpo $K^{(m)}$ stesso e gli altri precedenti pei quali il corrispondente Λ_i sia positivo, ponendo nel gruppo B i rimanenti, insieme a $K^{(m+1)} \dots K^{(\nu)}$. I due gruppi A, B soddisfano così alle condizioni del teorema α'), ed esiste quindi un' unità ε_m, di norma positiva, tale che dei suoi primi $\underline{m}$ logaritmi coniugati $l_{1m}, l_{2m}, \dots l_{mm}$ riescono positivi quelli del gruppo A e negativi quelli del gruppo B. Dopo ciò, è manifesto che nel secondo membro della (16) tutti i termini saranno positivi, o eventualmente nulli, ma non tutti nulli, e per ciò risulterà $\mathcal{L} > 0$ come si voleva. Il teorema β) è quindi stabilito.

§ 21.

Sistemi fondamentali di unità - Unità ridotte.

Prendiamo un sistema di $\nu-1$ unità

$$\varepsilon_1, \varepsilon_2, \dots \varepsilon_{\nu-1},$$

dotato delle proprietà espresse nel teorema β), e di cui sopra abbiamo accertata l'esistenza. Mediante queste $\nu-1$ unità, si generano infinite altre unità della forma

$$\eta = \varepsilon_1^{m_1} \varepsilon_2^{m_2} \dots \varepsilon_{\nu-1}^{m_{\nu-1}}, \tag{1}$$

facendo percorrere agli esponenti $m_1, m_2 \dots m_{\nu-1}$ tutti i valori razionali interi positivi, negativi o nulli. È facile vedere che queste infinite unità η sono tutte diverse fra loro, altrimenti esisterebbero degli esponenti razionali interi $r_1, r_2, \dots r_{\nu-1}$, non tutti nulli, pei quali risulterebbe

$$(2) \qquad \varepsilon_1^{r_1}\ \varepsilon_2^{r_2} \dots \varepsilon_{\nu-1}^{r_{\nu-1}} = 1\,,$$

ciò che vediamo subito essere impossibile. Come conseguenza della (1), avremmo infatti, per ogni valore dell'indice i da 1 a $\nu-1$

$$\left|\varepsilon_1^{(i)}\right|^{r_1} \left|\varepsilon_2^{(i)}\right|^{r_2} \dots \left|\varepsilon_{\nu-1}^{(i)}\right|^{r_{\nu-1}} = 1$$

e passando ai logaritmi

$$\left\{\begin{array}{l} r_1\, l_{11} + r_2\, l_{12} + \dots + r_{\nu-1}\, l_{1,\nu-1} = 0 \\ r_1\, l_{21} + r_2\, l_{22} + \dots + r_{\nu-1}\, l_{2,\nu-1} = 0 \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ r_1\, l_{\nu-1,1} + r_2\, l_{\nu-1,2} + \dots + r_{\nu-1}\, l_{\nu-1,\nu-1} = 0\,, \end{array}\right.$$

ciò che è contraddittorio col fatto che il determinante dei coefficienti $\mathcal{L}(\varepsilon_1, \varepsilon_2 \dots \varepsilon_{\nu-1})$ è diverso da zero. Non potendo dunque sussistere alcuna identità della forma (2), le $\nu-1$ unità $\varepsilon_1, \varepsilon_2 \dots \varepsilon_{\nu-1}$ sono appunto da dirsi fra loro indipendenti.

Vediamo ora come si comporta un'altra qualunque unità ε del corpo $K(\theta)$ rispetto a queste $\nu-1$. Intanto noi possiamo sempre determinare $\nu-1$ incognite $e_1, e_2 \dots e_{\nu-1}$, in un modo soltanto, in guisa da soddisfare alle ν equazioni

$$(3)\quad \begin{cases} e_1 l_{11} + e_2 l_{12} + \dots e_{\nu-1} l_{1,\nu-1} = l_1(\varepsilon) \\ e_1 l_{21} + e_2 l_{22} + \dots e_{\nu-1} l_{2,\nu-1} = l_2(\varepsilon) \\ \dots \dots \dots \dots \\ e_1 l_{\nu 1} + e_2 l_{\nu 1} + \dots e_{\nu-1} l_{\nu,\nu-1} = l_\nu(\varepsilon) \end{cases}$$

poichè, a causa della identità (14) § 20, la loro somma è identicamente soddisfatta, mentre le prime $\nu-1$ hanno il determinante $\mathfrak{L}(\varepsilon_1, \varepsilon_2 \dots \varepsilon_{\nu-1}) \neq 0$. Questi numeri reali $e_1, e_2 \dots e_{\nu-1}$, che fra breve vedremo essere numeri razionali, si diranno gli <u>esponenti</u> dell'unità ε rispetto al sistema $\mathfrak{S}$ di tutte le unità η della forma (1). Dalla definizione stessa di questi esponenti risulta che gli esponenti del prodotto di due unità ε, ε' si ottengono sommando gli esponenti corrispondenti di ε, ε', gli esponenti di ε^q (q intero qualunque) si hanno moltiplicando per q gli esponenti di ε, ecc. Manifestamente gli esponenti di un'unità η

del gruppo S dato dalla (1) sono appunto gli interi m_1, $m_2 \dots m_{\nu-1}$. Diremo equivalenti rispetto ad S due unità che differiscono per un fattore η del gruppo S: $\varepsilon' = \varepsilon\eta$; è chiaro che gli esponenti di due tali unità differiscono rispettivamente per numeri razionali interi, e viceversa ad ogni unità ε se ne potrà sostituire una equivalente aggiungendo o sottraendo a ciascun esponente e_i un intero arbitrario. In particolare, chiamando ridotta un' unità i cui esponenti e_i siano tutti positivi o nulli ma < 1, risulta di qui: ogni unità ε del corpo $K(\theta)$ è equivalente ad un' unità ridotta. Osserviamo che tra le unità ridotte si trovano certamente il numero 1 e tutte le eventuali unità di $K(\theta)$ che siano al tempo stesso radici m^{me} dell' unità ($\varepsilon^m = 1$), poichè in tal caso, tutti i moduli dei coniugati di ε essendo $= 1$, i secondi membri delle (3) e conseguentemente gli esponenti e_i sono tutti nulli.

In generale è facile vedere che: le unità ridotte in $K(\theta)$ sono in numero finito. Difatti se nelle (3) supponiamo che le e_i siano nell' intervallo $(0, 1)$, ne risultano le limitazioni

$$|\ell_1(\varepsilon)| \leq |t_{11}| + |\ell_{12}| + \cdots + |\ell_{1,\nu-1}|,\ |\ell_2(\varepsilon)| \leq |\ell_{21}| + |\ell_{22}| + \cdots + |\ell_{2,\nu-1}|, \cdots$$
$$|\ell_\nu(\varepsilon)| \leq |\ell_{\nu 1}| + |\ell_{\nu 2}| + \cdots |\ell_{\nu,\nu-1}|,$$

e per ciò anche i moduli di tutti i numeri coniugati con ε hanno limitazioni superiori, dipendenti solo da $(\varepsilon_1, \varepsilon_2 \cdots \varepsilon_{\nu-1})$. Ricorrendo al lemma a) § 18, si vede così subito che queste unità ridotte sono in numero finito.

Sia k il numero delle unità ridotte differenti in $K(\theta)$, e indichiamo con

$$(4) \qquad \rho_1, \rho_2, \cdots \rho_k$$

queste unità ridotte. Essendo ε una qualunque unità, le k unità

$$(5) \qquad \varepsilon\rho_1, \varepsilon\rho_2, \cdots \varepsilon\rho_k$$

sono equivalenti, in altro ordine, a $\rho_1, \rho_2, \cdots \rho_k$ giacchè due delle (5) non possono essere equivalenti fra loro (altrimenti sarebbero equivalenti e quindi eguali due corrispondenti ρ) e d'altronde ciascuna delle (5) trova la sua equivalente in una delle (4).

Il prodotto delle (5) differisce dunque dal prodotto delle (4) per un' unità η della forma (1) (del gruppo S) cioè: <u>Se k è il numero delle unità ridotte, la poten</u>

za ε^k di qualunque unità ε è un'unità η della forma $\eta = \varepsilon_1^{m_1}\,\varepsilon_2^{m_2}\ldots\varepsilon_{\nu-1}^{m_{\nu-1}}$.

Se indichiamo con $e_1, e_2 \ldots e_{\nu-1}$ gli esponenti di ε si ha in conseguenza

$$k e_1 = m_1 \;,\; k e_2 = m_2 \ldots k e_{\nu-1} = m_{\nu-1} \;,$$

onde si vede che: gli esponenti di qualunque unità sono numeri razionali con denominatore comune eguale al numero k delle unità ridotte.

Ciò premesso, prendiamo $\nu-1$ unità qualunque

$$\delta_1 \,,\, \delta_2 \ldots \delta_{\nu-1}$$

(indipendenti o no) e indichiamo con

$$e_{i1} \,,\, e_{i2} \ldots e_{i,\nu-1} \qquad (i = 1, 2 \ldots \nu-1)$$

gli esponenti di δ_i, onde avremo per le (3)

$$l_q(\delta_i) = \sum_{j=i}^{j=\nu-1} e_{ij}\, l_{qj} \qquad (i, q = 1, 2, \ldots \nu-1)$$

di qui, formando il determinante $L(\delta_1, \delta_2 \ldots \delta_{\nu-1}) = |l_q(\delta_i)|$, troviamo subito

$$(6) \qquad L(\delta_1, \delta_2, \ldots \delta_{\nu-1}) = \mathcal{E} . L(\varepsilon_1, \varepsilon_2, \ldots \varepsilon_{\nu-1}),$$

dove $\mathcal{E} = |e_{ik}|$ è il determinante degli esponenti delle δ. Queste saranno indipendenti se $\mathcal{E}$ non sarà nullo. Si osservi ora che, essendo le e_{ik} numeri razionali con denominatore k (eguale al numero delle unità ridotte), $\mathcal{E}$

stesso sarà della forma $\frac{N}{k^{\nu-1}}$ con N razionale intero; avremo quindi

$$(7) \qquad \mathfrak{L}(\delta_1, \delta_2 \cdots \delta_{\nu-1}) = \frac{N}{k^{\nu-1}} \mathfrak{L}(\varepsilon_1, \varepsilon_2, \cdots \varepsilon_{\nu-1}).$$

Cangiando il sistema di unità indipendenti $\delta_1, \delta_2 \ldots \delta_{\nu-1}$, varia soltanto il numero intero (positivo) N, e per uno almeno di questi sistemi N raggiungerà il minimo valore possibile. Un tale sistema di unità $\delta_1, \delta_2, \cdots \delta_{\nu-1}$, per il quale $\mathfrak{L}(\delta_1, \delta_2 \cdots \delta_{\nu-1})$ ha il minimo valore possibile, si dice un sistema fondamentale di unità. E qui avvertiamo che volendo comprendere nella ricerca anche le unità di norma negativa $= -1$ (ove ne esistano nel corpo), un sistema fondamentale potrà anche contenere unità di norma $= -1$.

§ 22.

Proprietà dei sistemi fondamentali - Il teorema finale di Dirichlet.

Possiamo supporre che il sistema di $\nu-1$ unità indipendenti $\varepsilon_1, \varepsilon_2 \cdots \varepsilon_{\nu-1}$ (di norma $= \pm 1$) sia già un sistema fondamentale. Cominciamo allora dal provare che una qualunque delle k unità ridotte avrà necessariamente esponenti $e_1, e_2 \cdots e_{\nu-1}$ tutti nulli.

Sia ρ una di queste unità ridotte e supponiamo al contrario che uno dei suoi esponenti per es. e_1 non sia nullo, e sia dunque $e_1 < 1$. Applichiamo la formola (6) alle $\nu-1$ unità

$$\delta_1 = \rho\,, \quad \delta_2 = \varepsilon_2\,, \ldots \delta_{\nu-1} = \varepsilon_{\nu-1}\,.$$

Qui il determinante $\mathcal{E}$ degli esponenti ha il valore

$$\begin{vmatrix} e_1 & e_2 & \ldots & e_{\nu-1} \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{vmatrix} = e_1 < 1\,,$$

e la (6) prova che $\mathcal{L}(\rho, \varepsilon_2 \ldots \varepsilon_{\nu-1}) < \mathcal{L}(\varepsilon_1\ \varepsilon_2 \ldots \varepsilon_{\nu-1})$, ciò che contraddice all'ipotesi che $\mathcal{L}(\varepsilon_1\ \varepsilon_2 \ldots \varepsilon_{\nu-1})$ abbia raggiunto il suo minimo valore.

Stabilita la proporzione enunciata, ne risulta l'importante conseguenza:

Se il sistema $(\varepsilon_1\ \varepsilon_2 \ldots \varepsilon_{\nu-1})$ è fondamentale, le k unità ridotte sono tutte e sole le radici k^{me} dell'unità. E infatti, per quanto si è visto al § precedente, ρ^k ha la forma $\varepsilon_1^{m_1}\ \varepsilon_2^{m_2} \ldots \varepsilon_{\nu-1}^{m_{\nu-1}}$, e siccome i suoi esponenti sono tutti nulli si ha $\rho^k = 1$; le unità ridotte essendo dunque un numero di k diverse sono tutte e sole le radi-

ci k^{me} dell'unità. Manifestamente poi non esiste nel corpo $K(\theta)$ alcuna altra unità che sia una radice m^{ma} di 1.

Se ricordiamo (§ 21) che qualunque unità del corpo $K(\theta)$ è equivalente ad un'unità ridotta, siamo arrivati così a stabilire il teorema capitale di Dirichlet:

Se per il corpo algebrico $K(\theta)$ è ν il numero complessivo, fra i corpi coniugati dei corpi reali e delle coppie di corpi immaginarii, esistono nel corpo $\nu-1$ unità fondamentali $\varepsilon_1\ \varepsilon_2 \dots \varepsilon_{\nu-1}$, ed un numero finito k di unità ρ radici m^e di 1, tali che si ottiene ogni altra unità ε del corpo componendo le potenze intere positive e negative di $\varepsilon_1\ \varepsilon_2 \dots \varepsilon_{\nu-1}$ colle k radici ρ, mediante la formola

$$(1) \qquad \varepsilon = \rho\, \varepsilon_1^{m_1}\ \varepsilon_2^{m_2} \dots \varepsilon_{\nu-1}^{m_{\nu-1}}.$$

Così, percorrendo ρ le k radici dell'unità contenute in $K(\theta)$, e dando agli esponenti $m_1, m_2 \dots m_{\nu-1}$ tutti i valori interi positivi, negativi o nulli, vengono rappresentate le unità del corpo, e ciascuna una sola volta.

Alla dimostrazione di questo teorema di Dirichlet, che costituisce una delle proprietà fondamentali nel

l'aritmetica generale dei corpi algebrici, facciamo ora seguire alcune osservazioni complementari.

Il teorema stesso può applicarsi tanto in senso stretto, alle sole unità ε di $N(\varepsilon) = +1$, quanto nel senso generale al complesso di tutte le unità comprendendovi anche quelle ε, se pure esistono nel corpo, per le quali invece $N(\varepsilon) = -1$.

Per quanto riguarda il sistema fondamentale (ε_1, $\varepsilon_2 \dots \varepsilon_{\nu-1}$), questo può cangiarsi in infiniti modi sostituendovi un altro sistema (δ_1, $\delta_2 \dots \delta_{\nu-1}$) tale che il determinante $\mathcal{E}$ dei relativi esponenti (§ 21)

$$\begin{vmatrix} e_{11} & e_{12} \dots & e_{1,\nu-1} \\ e_{21} & e_{22} \dots & e_{2,\nu-1} \\ \dots & \dots & \dots \\ e_{\nu-1,1} & e_{\nu-1,2} \dots & e_{\nu-1,\nu-1} \end{vmatrix}$$

sia eguale a $+1$. Con questo non varia il determinante $\mathcal{L}(\varepsilon_1, \varepsilon_2 \dots \varepsilon_{\nu-1})$, il cui valore è dunque una costante essenzialmente relativa al corpo e che dicesi, secondo Dedekind, il regolatore del corpo. Egualmente non varia il numero k delle unità ridotte (al variare del sistema fondamentale), perchè questo numero è sem-

pre quello delle radici m^{me} di 1 contenute nel corpo; ma se esistono nel corpo anche unità di $N(\varepsilon)=-1$, il numero k di tutte le unità ridotte è manifestamente il doppio di quello delle unità ridotte in senso stretto (con $N(\varepsilon)=+1$). In ogni caso il numero k di tutte le unità ridotte è pari, perchè soddisfano tutte all'equazione $x^k=1$ e d'altronde -1 è sempre insieme a $+1$ un'unità ridotta. Siccome poi, essendo n il grado del corpo, $N(-1)=(-1)^n$, si vede che -1 è un'unità ridotta in senso stretto solo quando il grado del corpo è pari.

Si osservi ora che dalle unità ε del corpo $K(\theta)$, date dalla (1), si passa alle unità dei corpi coniugati cangiando ciascun fattore del secondo membro nel relativo coniugato, e per ciò: il numero k di tutte le unità ridotte è lo stesso in tutti i corpi coniugati, ossia le unità ridotte sono comuni a tutti i corpi coniugati. Fra queste, appena $k>2$, soltanto ± 1, sono reali, e le rimanenti immaginarie non possono appartenere a corpi reali, dunque: se il numero di tutte le radici dell'unità contenute nel corpo è >2, tutti i corpi coniugati sono necessariamente immaginarii. In

un corpo reale, di radici dell'unità esistono solo le due ± 1. Di queste però, se n è impari, la seconda -1 ha la norma $N(-1) = -1$, onde segue: In ogni corpo di grado impari l'unica unità ridotta di norma $= +1$ è data da 1.

Esempio. – Per illustrare questi risultati generali di Dirichlet in un caso più semplice, prendiamo quello dei corpi quadratici reali, già accennato al § 14, ove avendosi $\nu = 2$ $(r = 2, s = 0)$ esiste una sola unità fondamentale. Limitandoci al caso $d \equiv 2, 3 \pmod 4$ (cfr. § 14), tutti i numeri interi del corpo sono della forma $x + y\sqrt{d}$ e la loro norma è $x^2 - dy^2$. La ricerca delle unità (diverse da ± 1) di norma positiva equivale alla risoluzione della equazione di Pell

$$t^2 - du^2 = 1.$$

Come caso particolare del teorema di Dirichlet risulta dunque la risolubilità in numeri interi positivi di questa equazione; quella a cui corrispondono i valori minimi positivi T, U per t, u dà l'unità fondamentale

$$\varepsilon_1 = T + U\sqrt{d}$$

e tutte le altre si ottengono dalla formula $\varepsilon = \pm\, \varepsilon_1^r$

$r = 0, \pm 1, \pm 2, \dots$

Nel caso che esistano anche unità di norma $= -1$ (delle soluzioni dell'equazione $t^2 - du^2 = -1$) l'unità fondamentale è quella che corrisponde alla minima sua soluzione in interi positivi, e dalla formula precedente si hanno ancora tutte le unità del corpo, quelle a norma positiva per r pari, quelle a norma negativa per r dispari.

Gli altri casi in cui, secondo il teorema di Dirichlet, si ha una sola unità fondamentale, pei quali cioè $\nu = 2$, corrispondono a

$r = 1, \ s = 1$, corpo cubico (con un corpo reale e due complessi coniugati)

$r = 0, \ s = 2$ corpo biquadratico (con due coppie di corpi complessi coniugati).

Capitolo II.

Ideali nei corpi algebrici - Moltiplicazione e divisibilità - Risoluzione unica in ideali primi - Congruenze rispetto ad ideali - Equivalenza - Classi di ideali - Forme decomponibili coordinate - Corpi di Galois - Corpi circolari.

§ 23

Ideali nei corpi algebrici. Loro basi.

Abbiamo già descritto, sull'esempio particolare dei corpi quadratici del § 7 (cfr. anche § 13), il fenomeno nuovo che si presenta in generale nell'aritmetica (teoria dei numeri interi) dei corpi algebrici: della separazione fra il concetto di numero indecomponibile e quello di fattore primo, al quale è legato l'altro che sebbene nei corpi finiti la decomponibilità dei numeri nel senso del § 13, sia limitata, essa non è più unica. Ed anche abbiamo detto come que-

ste difficoltà siano state completamente vinte da Kummer e Dedekind, colla creazione della teoria degli <u>ideali</u>, che ha permesso di ristabilire, nell'aritmetica dei corpi algebrici, le leggi della divisibilità dell'ordinaria aritmetica. Ora ci volgiamo appunto a descrivere i principii fondamentali di questa teoria.

Consideriamo un determinato corpo algebrico $K(\theta)$ di grado n, e per numeri intendiamo dei <u>numeri interi</u> del corpo. Diremo che un sistema J di infiniti di questi numeri forma un ideale del corpo $K(\theta)$, quando sono soddisfatte le due leggi fondamentali seguenti:

I) <u>la somma o la differenza di due numeri qualunque di J è ancora un numero di J.</u>

II) <u>il prodotto di un numero qualunque di J per ogni intero arbitrario del corpo appartiene ad J.</u>

Da queste due leggi elementari segue che, se dall'ideale J si estrae un numero qualunque q di numeri $\alpha_1, \alpha_2 \dots \alpha_q$, e si moltiplicano rispettivamente per q interi arbitrarii $\lambda_1, \lambda_2 \dots \lambda_q$ del corpo $K(\theta)$, la somma

$$\lambda_1\alpha_1 + \lambda_2\alpha_2 + \dots + \lambda_q\alpha_q$$

appartiene ancora all'ideale J.

Viceversa, se si prendono q interi fissi arbitrarii di $K(\theta)$ non tutti nulli siano $\alpha_1, \alpha_2 \dots \alpha_q$, e si considerano tutti i numeri della forma

$$(1) \qquad \alpha = \lambda_1\alpha_1 + \lambda_2\alpha_2 + \dots + \lambda_q\alpha_q ,$$

dove i numeri λ percorrono gli interi del corpo, questi numeri α costituiscono un ideale J; poichè infatti un tale sistema (1) di numeri soddisfa alle due leggi elementari I) e II). L'ideale (1) essendo generato dai numeri fissi (arbitrarii) $\alpha_1, \alpha_2 \dots \alpha_q$, sarà indicato colla notazione

$$J = (\alpha_1, \alpha_2, \dots \alpha_q).$$

In generale, nel seguito, gli ideali del corpo si indicheranno con lettere majuscole $A, B, \dots$

Un ideale A che si può generare con un solo numero α del corpo dicesi ideale principale e si scrive

$$A = (\alpha).$$

Affinchè due ideali

$$A = (\alpha_1, \alpha_2 \cdots \alpha_q) \quad , \quad B = (\beta_1, \beta_2 \cdots \beta_q)$$

siano eguali (constino degli stessi numeri), è manifestamente necessario e sufficiente che siano soddisfatte le due condizioni seguenti:

a) ciascuno dei q numeri α appartenga a B, cioè sia

$$\alpha_i = \sum_{k=1}^{k=s} \lambda_{ik} \beta_k \qquad (i = 1, 2, \cdots q),$$

dove i moltiplicatori λ_{ik} sono interi di $K(\theta)$.

b) ciascuno degli s numeri β appartenga ad A, cioè

$$\beta_j = \sum_{l=1}^{l=q} \mu_{jl} \alpha_l ,$$

i moltiplicatori μ_{jl} essendo interi di $K(\theta)$.

In particolare, due ideali principali (α), (β) sono eguali allora ed allora soltanto che α è multiplo di β e nello stesso tempo β multiplo di α, cioè:

<u>Due ideali principali (α), (β) sono eguali solo quando i due numeri α, β sono associati (differiscono per una unità</u>).

L'ideale principale, generato dal numero 1, o da qualunque altra unità, consta manifestamente di <u>tutti</u> gli interi del corpo e prende il nome di <u>ideale unità</u>; lo indicheremo con O.

Si osservi che nella designazione di un ideale

$$J = (\alpha_1, \alpha_2, \cdots \alpha_q),$$

si possono sopprimere quei numeri α_i che risultassero nulli e, se si presentano più α eguali, basta conservarne uno solo.

Dopo queste ovvie osservazioni sugli ideali, passiamo a stabilire una nozione importante quella della base di un ideale, già introdotta al § 12 per il complesso di tutti gli interi del corpo, cioè per l'ideale unità O. In primo luogo è immediata la proposizione:

<u>In ogni ideale A del corpo finito $K(\theta)$ di grado n possono sempre scegliersi, ed in infiniti modi, n numeri fra loro indipendenti.</u>

E infatti prendiamo una qualunque base $\omega_1, \omega_2, \ldots \omega_n$ del corpo $K(\theta)$ (§ 12), e dall'ideale A estragghiamo ad arbitrio un numero α; allora gli n numeri

$$\alpha\omega_1, \alpha\omega_2, \ldots \alpha\omega_n$$

appartengono (per la proprietà fondamentale II)) all'ideale A, e sono indipendenti, come $\omega_1, \omega_2, \ldots \omega_n$ (§ 11).

Se ora $\alpha_1, \alpha_2, \ldots \alpha_n$ è un qualunque sistema di n numeri indipendenti dell'ideale A, esprimendoli per la base $\omega_1, \omega_2, \ldots \omega_n$ di $K(\theta)$ (cioè di O), avremo

$$\alpha_i = \sum_{k=1}^{k=n} a_{ik}\,\omega_k \qquad (i = 1, 2, \ldots n), \text{ (a_{ik} numeri razionali interi)},$$

onde risulta

$$(2) \qquad \Delta(\alpha_1\, \alpha_2 \ldots \alpha_n) = |a_{ik}|^2 \Delta(\omega_1\, \omega_2 \ldots \omega_n).$$

Il discriminante $\Delta(\alpha_1, \alpha_2 \ldots \alpha_n)$ degli n numeri di A differisce dal numero fondamentale D del corpo pel quadrato del numero razionale intero

$$\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix},$$

e fra gli infiniti sistemi di n numeri indipendenti in A ve ne saranno dunque di quelli pei quali $|\Delta(\alpha_1, \alpha_2 \ldots \alpha_n)|$ riceve il valore minimo possibile. Supponiamo che sia già $\alpha_1, \alpha_2 \ldots \alpha_n$ un tale sistema, e dimostriamo che allora:

Qualunque numero α dell'ideale A sarà dato dalla formula

$$(I) \qquad \alpha = h_1\alpha_1 + h_2\alpha_2 + \ldots + h_n\alpha_n$$

con numeri $h_1, h_2, \ldots h_n$ razionali interi.

E infatti, siccome $\alpha_1, \alpha_2, \ldots \alpha_n$ sono indipendenti, qualunque numero α di A si può certamente scrivere sotto la forma (I) colle h numeri razionali; ma ora proviamo che queste h sono necessariamente in-

teri. Supponiamo, al contrario, che per es. h_1 non sia intero e scriviamo

$$h_1 = q_1 + r$$

con q_1 intero e r frazione propria $0 < r < 1$. Il numero $\alpha' = \alpha - q_1\alpha_1 = r_1\alpha_1 + h_2\alpha_2 + \cdots h_n\alpha_n$ appartiene all'ideale A e si ha

$$\Delta(\alpha', \alpha_2, \cdots \alpha_n) = \begin{vmatrix} r & h_2 \cdots h_n \\ 0 & 1 \cdots 0 \\ 0 & 0 \cdots 1 \end{vmatrix}^2 \Delta(\alpha_1, \alpha_2 \cdots \alpha_n) = r^2 \Delta(\alpha_1, \alpha_2 \cdots \alpha_n),$$

e siccome $r < 1$, si avrebbe $|\Delta(\alpha', \alpha_2 \cdots \alpha_n)| < |\Delta(\alpha_1 \alpha_2 \cdots \alpha_n)|$, contro l'ipotesi che $|\Delta(\alpha_1, \alpha_2 \cdots \alpha_n)|$ abbia già raggiunto il suo minimo.

Concludiamo quindi: <u>In ogni ideale A si possono (in infiniti modi) scegliere n numeri $\alpha_1, \alpha_2, \ldots \alpha_n$, in modo che ogni altro numero α dell'ideale si ponga sotto la forma (I)</u>

$$\alpha = h_1\alpha_1 + h_2\alpha_2 + \cdots + h_n\alpha_n$$

<u>coi coefficienti h razionali interi.</u>

Diremo per ciò che questi n numeri $\alpha_1, \alpha_2 \cdots \alpha_n$ costituiscono una base dell'ideale A, e scriveremo

$$A = [\alpha_1, \alpha_2 \cdots \alpha_n]$$

Naturalmente la base di un ideale si può variare in infiniti modi e come al § 12 per l'ideale unità 0, si vede subito che da una base $[\alpha_1, \alpha_2 \dots \alpha_n]$ dell'ideale A si passa a qualunque altra $[\alpha'_1, \alpha'_2 \dots \alpha'_n]$ eseguendo una sostituzione

$$\alpha'_i = \sum_{k=1}^{k=n} c_{ik} \alpha_k$$

a coefficienti c_{ik} razionali interi e determinante $|c_{ik}| = \pm 1$.

Si osserverà che, in qualunque modo si formi la base dell'ideale A, il discriminante $\Delta(\alpha_1, \alpha_2 \dots \alpha_n)$ della base resta sempre lo stesso e, a causa della formula (2), il suo quoziente pel numero fondamentale D del corpo è il quadrato di un numero intero. Questo numero intero $\sqrt{\frac{\Delta(\alpha_1, \alpha_2 \dots \alpha_n)}{D}}$ ha per l'ideale un significato importantissimo che impareremo subito a conoscere (norma dell'ideale).

Intanto se A è un ideale principale: $A = (\alpha)$, questo significato si riconosce subito, perchè allora ogni numero di A, in particolare quelli della base, sono divisibili per α

$$\alpha_1 = \beta_1 \alpha \quad , \quad \alpha_2 = \beta_2 \alpha \ , \ \dots \ \alpha_n = \beta_n \alpha \ ,$$

, e siccome sopprimendo via tutti i numeri di A il fattore α si ottengono tutti gli interi, i numeri $\beta_1, \beta_2 \dots \dots \beta_n$ formano una base del corpo (dell'ideale unità) ed è quindi

$$\Delta(\beta_1, \beta_2, \dots \beta_n) = \mathfrak{D}.$$

Dalle formule superiori si ha ora

$$\Delta(\alpha_1, \alpha_2 \dots \alpha_n) = \left(N(\alpha)\right)^2 \cdot \mathfrak{D},$$

cioè

$$\sqrt{\frac{\Delta(\alpha_1, \alpha_2 \dots \alpha_n)}{\mathfrak{D}}} = |N(\alpha)|$$

§ 24

Congruenza dei numeri rispetto ad ideali.
Norma di un ideale.

Nella teoria degli ideali i numeri stessi α del corpo sono, in certo senso, sostituibili dagli ideali principali corrispondenti (α), e in molte questioni accade che nozioni relative ai numeri possono generalizzarsi agli ideali in generale, trasportandole prima dai numeri ai corrispondenti ideali principali, poi da questi a tutti gli ideali.

Un primo ed importante esempio si offre nella

nozione di congruenza dei numeri rispetto ad un modulo. Come nell'ordinaria aritmetica, così in quella degli interi algebrici in generale, noi diciamo due numeri interi β, γ congrui rispetto ad un terzo α quando la differenza $\beta-\gamma$ è divisibile per α, cioè quando $\beta-\gamma$ appartiene all'ideale principale (α), e scriviamo $\beta \equiv \gamma$ [mod (α)]. E allora definiamo la congruenza di numeri nel corpo $K(\theta)$ rispetto ad un ideale *qualunque* A nel modo seguente:

Due interi β, γ del corpo $K(\theta)$ si dicono congruenti fra loro rispetto all'ideale A quando la differenza $\beta-\gamma$ appartiene ad A. Per significare questa congruenza si adotta la scrittura

$$\beta \equiv \gamma \pmod{A} \quad [\text{od anche } \beta \equiv \gamma\, (A)].$$

In particolare $\beta \equiv 0 \pmod{A}$ significa che β è un numero di A; ed allora si dice anche che il numero β è *divisibile* per l'ideale A [l'ideale principale (β) per l'ideale A].

Dalle proprietà elementari dei numeri algebrici, e dalla definizione degli ideali, risulta che su queste congruenze, rispetto ad un ideale fisso A, si può

operare come sulle congruenze dell'aritmetica razionale per somma, sottrazione e moltiplicazione, onde vale in generale il principio seguente: Se $f(x, y, z \dots)$ denota una funzione razionale intera delle variabili $x, y, z, \dots$ con coefficienti interi nel corpo $K(\theta)$ e per $x, y, z, \dots$ si sostituiscono due sistemi di valori interi $(\alpha, \beta, \gamma, \dots)$, $(\alpha', \beta', \gamma' \dots)$, rispettivamente congrui fra loro rispetto ad un ideale A, anche i valori assunti da $f(x, y, z, \dots)$ sono congrui fra loro, cioè da

$$\alpha' \equiv \alpha \ , \quad \beta' \equiv \beta \ , \quad \gamma' \equiv \gamma \dots \qquad (\mathrm{mod}\ A)$$

segue $f(\alpha', \beta', \gamma' \dots) \equiv f(\alpha, \beta, \gamma \dots) \ (\mathrm{mod}\ A)$.

Ripartiamo allora, rispetto all'ideale A, i numeri interi del corpo $K(\theta)$ in classi, ponendo nella medesima classe quelli che sono congrui con uno stesso numero, indi fra loro, dimostriamo che il numero delle classi è finito, cioè: nel corpo $K(\theta)$ esiste soltanto un numero finito di numeri interi incongrui fra loro $(\mathrm{mod}\ A)$. Questo numero intero razionale positivo prende il nome di norma dell'ideale A e si indica con $N_m(A)$, o anche $N(A)$.

Per dimostrare questo, e calcolare effettivamente

$N(A)$, noi ridurremo la questione a quella già risoluta al § 15 per il numero delle classi delle forme lineari rispetto ad un dato sistema di forme. L'identità dei due problemi è resa in effetto palese dalle considerazioni seguenti. Dell'ideale A prendiamo una base $[\alpha_1, \alpha_2, \dots \alpha_n]$, e siano

$$(1) \qquad \alpha_i = \sum_{k=1}^{k=n} a_{ik}\, \omega_k \qquad (i = 1, 2 \dots n)$$

le formole che esprimono questa base di A per la base $[\omega_1, \omega_2, \dots, \omega_n]$ di $K(\theta)$, cioè dell'ideale unità O. In questa formola (1), i coefficienti a_{ik} sono razionali interi e il determinante $|a_{ik}|$, diverso da zero, può senza altro supporsi positivo, chè in caso contrario basterebbe cangiare per es. α_1 in $-\alpha_1$. Ora due numeri qualunque β, ρ di O si scrivono, in modo unico sotto la forma

$$\beta = c_1 \omega_1 + c_2 \omega_2 + \dots + c_n \omega_n$$

$$\rho = c'_1 \omega_1 + c'_2 \omega_2 + \dots + c'_n \omega_n$$

coi coefficienti c, c' razionali interi e la congruenza $\beta \equiv \rho \pmod{A}$ significa che $\beta - \rho$ è un numero di A, cioè della forma $k_1\alpha_1 + k_2\alpha_2 + \dots + k_n\alpha_n$ (k_i interi razionali); abbiamo quindi, se $\beta \equiv \rho \pmod{A}$:

$$c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n = c_1'\omega_1 + c_2'\omega_2 + \cdots + c_n'\omega_n + h_1\sum_k a_{1k}\omega_k + \cdots + h_n\sum_k a_{nk}\omega_k$$

e questa, a causa della indipendenza delle ω_i, deve essere un'identità. Se dunque sostituiamo ad $\omega_1, \omega_2, \cdots \omega_n$ delle variabili indipendenti x, i numeri α_i si cangiano nelle $\underline{n}$ forme lineari

$$f_i = \sum_k a_{ik} x_k \qquad (i = 1, 2, \cdots n)$$

e i due numeri β, γ nelle forme $\varphi = \sum_k c_k x_k$, $\psi = \sum_k c_k' x_k$. La congruenza $\beta \equiv \gamma \pmod{A}$ equivale così perfettamente, secondo le nozioni del § 15, alla congruenza di forme lineari

$$\varphi \equiv \psi \quad (\text{modd } f_1, f_2, \cdots f_n),$$

poichè questa segue, come si è visto, dalla prima, e la inversa è evidente. Il numero dei numeri di $\mathfrak{O}$ incongrui $(\text{mod } A)$ eguaglia dunque il numero delle classi delle forme lineari (a coefficienti razionali interi) rispetto al sistema delle n forme fondamentali $f_1, f_2, \cdots f_n$. Ma si è trovato, al § 15, che quest'ultimo numero è dato dal valore (positivo) del determinante $|a_{ik}|$, onde resta stabilito il nostro enunciato insieme al significato di questo determinante, come norma dell'ideale A.

Così abbiamo: rispetto all'ideale A, il numero dei numeri interi in $K(\theta)$, che sono fra loro incongrui (mod A) è finito ed eguaglia il determinante $|a_{ik}|$ della sostituzione lineare (1) che esprime la base di A per la base del corpo.

Esprimendo pei discriminanti delle basi, siccome

$$\Delta(\alpha_1, \alpha_2, \dots \alpha_n) = |a_{ik}|^2 \Delta(\omega_1, \omega_2, \dots \omega_n) = |a_{ik}|^2 \cdot D,$$

ne risulta per la norma $N(A)$ dell'ideale, che dà appunto il numero di quei numeri incongrui, la formola:

$$\text{(I)} \qquad N(A) = \sqrt{\frac{\Delta(\alpha_1, \alpha_2, \dots \alpha_n)}{D}}$$

(D numero fondamentale di $K(\theta)$).

In particolare, se si confronta questa formola con quella finale del § precedente, relativa al caso di un ideale (α) principale, risulta:

La norma di un ideale principale eguaglia il valore assoluto della norma del numero generatore (prodotto dei numeri coniugati), in simboli.

$$N((\alpha)) = |N\alpha|.$$

È manifesto poi da queste formole (e del resto di immediata evidenza a priori) che:

L'unico ideale di norma $N(A)=1$ è l'ideale unità 0.

Notiamo in fine che, dal procedimento usato al § 15 per costruire un sistema di forme lineari incongrue (modd $f_1, f_2, \cdots f_n$), risulta che si possono per un ideale A costituire basi della forma particolare seguente:

$$(2)\quad \begin{cases} \alpha_1 = c_{11}\,\omega_1 \\ \alpha_2 = c_{21}\,\omega_1 + c_{22}\,\omega_2 \\ \alpha_3 = c_{31}\,\omega_1 + c_{32}\,\omega_2 + c_{33}\,\omega_3 \\ \cdots\cdots\cdots\cdots \\ \alpha_n = c_{n1}\,\omega_1 + c_{n2}\,\omega_2 + \cdots + c_{nn}\,\omega_n \end{cases},$$

dove in generale c_{mm} (per $m=1,2,\cdots n$) indica il minimo intero positivo pel quale esiste in $K(\theta)$ un numero α_m della forma $\alpha_m = c_{m1}\,\omega_1 + c_{m2}\,\omega_2 + \cdots + c_{mm}\,\omega_m$, dove anche le antecedenti $c_{m1}, \cdots, c_{m,m-1}$ sono numeri razionali interi. Le speciali basi della forma (2) si diranno basi ridotte; per una siffatta base si ha manifestamente

$$N(A) = c_{11}\,c_{22}\cdots c_{nn}.$$

Moltiplicazione degli ideali. - Conversione in ideali principali.

Delle operazioni elementari sui numeri (interi) del corpo la somma e la sottrazione non sono suscettibili di estendersi, nel senso sopra spiegato, ai nuovi enti agli ideali. Ma è molto importante che invece l'altra operazione elementare la moltiplicazione può estendersi agli ideali. Se (α), (β) sono due ideali principali diciamo loro prodotto l'ideale principale (ρ) generato dal numero $\alpha\beta$. Prendiamo ora due ideali qualunque A, B dati, sotto la forma primitiva del § 23, come individuati dai loro numeri generatori:

$$(1) \qquad A = (\alpha_1, \alpha_2, \cdots \alpha_q), \quad B = (\beta_1, \beta_2, \cdots \beta_s),$$

e consideriamo i qs numeri $\alpha_i \beta_k$ $(i = 1, 2, \cdots q,\ k = 1, 2, \cdots s)$; questi generano a loro volta un terzo ideale $C = (\alpha_1\beta_1, \cdots \alpha_1\beta_s;\ \alpha_2\beta_1, \cdots \alpha_2\beta_s;\ \cdots \alpha_q\beta_1, \cdots \alpha_q\beta_s)$, che si dirà il prodotto dei due ideali A e B e si scriverà

$$C = AB.$$

Si ha dunque per definizione

$$(\alpha_1, \alpha_2 \cdots \alpha_q) \cdot (\beta_1, \beta_2 \cdots \beta_s) = (\alpha_1\beta_1, \cdots \alpha_1\beta_s; \alpha_2\beta_1, \cdots \alpha_2\beta_s, \cdots \alpha_q\beta_1, \cdots \alpha_q\beta_s).$$

ogni numero ρ dell'ideale prodotto ha la forma

$$(2) \qquad \rho = \sum_{i=1}^{i=q} \sum_{k=1}^{k=s} \lambda_{ik} \alpha_i \beta_k \ ,$$

i numeri λ_{ik} percorrendo tutti gli interi di $K(\theta)$. In particolare si osservi che: nell'ideale prodotto AB è contenuto ogni prodotto di un numero di A per un numero di B.

Importa ora osservare, per giustificare la definizione precedente, che in effetto l'ideale prodotto è indipendente dal modo (1) di generazione dei due ideali A, B, e cioè se

$$\begin{cases} (\alpha_1, \alpha_2 \cdots \alpha_q) = (\alpha'_1, \alpha'_2 \cdots \alpha'_{q'}) \\ (\beta_1, \beta_2 \cdots \beta_{q'}) = (\beta'_1, \beta'_2 \cdots \beta'_{s'}) \end{cases} ,$$

è anche

$$(3) \qquad (\alpha_1, \alpha_2 \cdots \alpha_q) \cdot (\beta_1, \beta_2 \cdots \beta_s) = (\alpha'_1, \alpha'_2 \cdots \alpha'_{q'}) \cdot (\beta'_1, \beta'_2, \cdots \beta'_{s'}) .$$

Difatti, siccome

$$\alpha'_i = \sum_{r=1}^{r=q} \mu_{ir} \alpha_r \quad , \quad \beta'_j = \sum_{t=1}^{t=s} \lambda_{jt} \beta_t$$

con μ_{ir}, λ_{jt} interi di $K(\theta)$, così è anche

$$\alpha'_i \beta'_j = \sum_{r=1}^{r=q} \sum_{t=1}^{t=s} \mu_{ir} \lambda_{jt} \alpha_r \beta_t$$

un numero ρ della forma (2), cioè dell'ideale a sinistra in (3), e medesimamente qualunque $\alpha_i \beta_k$ appartiene all'ideale a destra in (3).

Dalla definizione stessa che abbiamo dato per il prodotto di due ideali, simmetrica rispetto a questi

due ideali, risulta subito che vale la proprietà <u>commutativa</u>

$$BA = AB.$$

La definizione si estende manifestamente al prodotto di più ideali, così per tre ideali A, B, C se

$$A = (\alpha_1, \alpha_2 \dots \alpha_q), \quad B = (\beta_1, \beta_2 \dots \beta_s), \quad C = (\gamma_1, \gamma_2, \dots \gamma_r),$$

sarà

$$ABC = (\dots, \alpha_i \beta_k \gamma_l, \dots) \begin{cases} i = 1, 2, \dots q \\ k = 1, 2, \dots s \\ l = 1, 2, \dots r \end{cases}$$

Vale pel prodotto di quanti si vogliano ideali, colla legge commutativa anche l'associativa, ed è chiaro cosa debba intendersi per potenza A^m di un ideale con esponente intero e positivo. A causa della legge associativa, vale per prodotti di potenze di uno stesso ideale A la legge di sommazione degli esponenti: $A^m \cdot A^{m'} = A^{m+m'}$.

Ora, ritornando alla definizione del prodotto di due ideali, osserviamo che ogni numero γ dell'ideale prodotto si può scrivere per la (2)

$$\gamma = \sum_{i=1}^{i=q} \alpha_i \left(\sum_{k=1}^{k=s} \lambda_{ik} \beta_k \right)$$

e siccome $\eta_i = \sum_{k=1}^{k=s} \lambda_{ik} \beta_k$ è un numero di $K(\theta)$, anzi di B,

ne segue che $\mu = \sum_{i=1}^{i=r} \eta_i \alpha_i \gamma_i$ appartiene ad A, e per la ragione analoga a B: *Ogni numero dell'ideale prodotto di più ideali appartiene a ciascuno degli ideali fattori.*

Andiamo ora a dimostrare un teorema di fondamentale importanza per la teoria, che si enuncia:

A) *Qualunque ideale A può convertirsi, moliplicandolo per un conveniente ideale B, in un ideale AB che sia principale ed anzi in un ideale (δ) generato da un numero razionale intero e positivo δ.*

La dimostrazione si fonda sul teorema finale (δ) al § 10 e sulle osservazioni seguenti.

Siano $\alpha_0, \alpha_1, \ldots \alpha_m$ numeri generatori dell'ideale

$$A = (\alpha_0, \alpha_1, \alpha_2, \ldots \alpha_m),$$

al quale associamo il polinomio di grado m in una variabile x

$$A(x) = \alpha_0 x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m .$$

Poniamo i coefficienti α, interi di $K(\theta)$, sotto la rispettiva forma normale § 11

$$\alpha_0 = r_0(\theta), \; \alpha_1 = r_1(\theta), \ldots \alpha_m = r_m(\theta)$$

e consideriamo in pari tempo tutti i loro coniugati, che

saranno pure interi (dei corpi coniugati):

$$\alpha_0^{(i)} = r_0(\theta^{(i)}), \quad \alpha_1^{(i)} = r_1(\theta^{(i)}) \ldots \alpha_m^{(i)} = r_m(\theta^{(i)}), \quad (i = 1, 2, \ldots n)$$

e costruiamo il polinomio in x di grado mn.

$$C(x) = \prod_{i=1}^{i=n} \left\{ \alpha_0^{(i)} x^m + \alpha_1^{(i)} x^{m-1} + \cdots + \alpha_m^{(i)} \right\} = c_0 x^{mn} + c_1 x^{mn-1} + \cdots + c_{mn}.$$

Questo polinomio $C(x)$ contiene manifestamente come (primo) fattore $A(x)$; i suoi coefficienti sono interi algebrici, come combinazioni intere degli $\alpha^{(i)}$, anzi essendo formati con questi in modo simmetrico saranno razionali, come deriva dal teorema sulle funzioni simmetriche, o da ciò che ciascuno di questi numeri è uguale a tutti i suoi coniugati. Il polinomio $C(x)$ è divisibile, come si è detto, per $A(x)$ e se poniamo

$$C(x) = A(x)\,B(x),$$

sarà $B(x)$ di grado $q = m(n-1)$, poniamo

$$B(x) = \beta_0 x^q + \beta_1 x^{q-1} + \cdots + \beta_q.$$

Questi coefficienti β, ottenendosi $B(x)$ coll'algoritmo della divisione di $C(x)$ per $A(x)$, apparterranno al corpo $K(\theta)$ come quelli di $A(x)$, e saranno di più interi, avendosi

$$B(x) = \prod_{i=2}^{i=n} \left\{ \alpha_0^{(i)} x^m + \alpha_1^{(i)} x^{m-1} + \cdots + \alpha_m^{(i)} \right\}$$

ed essendo interi tutti i numeri $\alpha^{(i)}$.

Dopo ciò associamo al polinomio $B(x)$ l'ideale

$$B = (\beta_0, \beta_1, \beta_2 \cdots \beta_q),$$

e dimostriamo che questo soddisfa alla condizione voluta $AB = (\delta)$.

Indichiamo per ciò con δ il massimo comun divisore degli interi razionali

$$c_0, c_1, \cdots c_{mn},$$

ed applichiamo il ricordato teorema δ) § 10. Siccome δ divide tutti i coefficienti c, dividerà anche ogni prodotto

$$\alpha_i \beta_k \quad \begin{cases} i = 0, 1, \cdots m \\ k = 0, 1, \cdots q, \end{cases}$$

onde ogni numero di AB sarà intanto divisibile per δ, e resta soltanto da provare che AB contiene δ, indi consta di tutti i multipli di δ. Si ricordi per ciò che δ è il massimo comun divisore dei numeri razionali interi $c_0, c_1, c_2, \cdots c_{mn}$, ed è quindi solubile in numeri razionali interi $C_0, C_1 \cdots C_{mn}$ l'equazione

$$\delta = C_0 c_0 + C_1 c_1 + \cdots + C_{mn} c_{mn};$$

ma allora, siccome ciascun coefficiente c è la somma di prodotti della forma $\alpha_i \beta_k$, anche δ è una combina-

zione lineare intera (a coefficienti razionali interi) di tali prodotti, ed è quindi un numero dell'ideale AB, c. d. d.

Dal teorema principale A) così dimostrato cominciamo subito a dedurre alcune congruenze, e prima notiamo il teorema

a) Se gli ideali A, B, C sono tali che si abbia

$$(4) \qquad AB = AC,$$

allora è necessariamente $B = C$.

Secondo il teorema A), si prenda un quarto ideale D tale che sia $AD = (\delta)$ e si moltiplichi la supposta eguaglianza per (δ) onde risulta

$$(4^*) \qquad (\delta).B = (\delta).C$$

e il teorema a) da dimostrarsi è così ridotto al caso in cui nella (4) l'ideale moltiplicatore A sia il principale (δ). Ora, se β è un numero qualunque di B e γ uno di C, l'ideale a sinistra in (4^*) consta di tutti i numeri della forma $\delta\beta$, quello a destra di tutti i numeri della forma $\delta\gamma$, e dalla coincidenza dei due ideali risulta, dividendo tutti questi numeri per δ, che si ha $B = C$.

Si è già osservato sopra che, se un ideale C può risolversi nel prodotto dell'ideale A per un altro ideale B, allora ogni numero ρ di C appartiene all'ideale divisore A. Ora, mediante il teorema principale $A)$, siamo in grado di invertire questa proposizione e dimostrare dunque:

$b)$ La condizione necessaria e sufficiente affinchè un ideale C ammetta l'ideale A per divisore (possa risolversi in $C = AB$) è che ogni numero ρ di C appartenga ad A. – Che sia necessaria si è visto, e per dimostrare che è sufficiente pongasi

$$A = (\alpha_1, \alpha_2, \dots \alpha_r) \qquad C = (\rho_1, \rho_2, \dots \rho_s),$$

e si determini, secondo il teorema principale $A)$, un ideale B tale che si abbia

$$AB = (\delta),$$

e scriviamo

$$B = (\beta_1, \beta_2 \dots \beta_r).$$

Ogni numero di CB è una combinazione lineare, con coefficienti interi in $K(\theta)$, dei prodotti $\rho_i \beta_j$, e siccome, per ipotesi, ciascun numero di C in particolare ρ_i trovasi in A, così ρ_i è alla sua volta una

combinazione lineare di $\alpha_1, \alpha_2, \dots \alpha_q$ (con coefficienti interi in $K(\theta)$), onde si vede che qualunque numero di CB è una combinazione lineare, con coefficienti interi in $K(\theta)$, dei prodotti $\alpha_i \beta_j$, cioè ogni numero di CB è anche un numero di AB. Essendo $AB = (\delta)$, tutti i numeri di AB, in particolare quelli di CB, sono divisibili per δ. Scrivendo dunque CB mediante numeri generatori, diciamo in numero di t, avremo

$$CB = (\delta\varepsilon_1, \delta\varepsilon_2, \dots \delta\varepsilon_t),$$

con $\varepsilon_1, \varepsilon_2, \dots \varepsilon_t$ interi. L'ideale CB è dunque il prodotto dell'ideale principale (δ) per l'ideale $(\varepsilon_1, \varepsilon_2, \dots \varepsilon_t)$, ossia

$$CB = (\delta) \cdot (\varepsilon_1, \varepsilon_2, \dots \varepsilon_t),$$

e siccome $(\delta) = AB$ possiamo anche scriviamo

$$BC = B \cdot A(\varepsilon_1, \varepsilon_2, \dots \varepsilon_t),$$

da cui, applicando il teorema a) risulta

$$C = A \cdot (\varepsilon_1, \varepsilon_2, \dots \varepsilon_t).$$

Questa dimostra appunto che C si risolve nel prodotto dell'ideale A per un altro ideale, c. d. d.

Divisibilità degli ideali - Ideali primi - Decomponibilità unica in fattori primi.

I risultati fondamentali ottenuti nel § precedente ci consentono di porre la definizione di <u>divisibilità</u> degli ideali, della loro decomposizione in fattori (ideali) primi ecc. nella qual cosa, come si vedrà, tutte le leggi dell'aritmetica razionale per la decomposizione dei numeri risulteranno perfettamente ristabilite.

Diciamo che un ideale A è <u>divisibile</u> per l'ideale B, o che B <u>è un divisore di A</u>, quando A può risolversi nel prodotto di B per un terzo ideale C.

Secondo il teorema b) superiore condizione necessaria e sufficiente affinchè A sia divisibile per B è che ogni numero di A si trovi anche in B, onde potrebbe assumersi come equivalente quest'altra definizione:

α) <u>Un ideale A è divisibile per un ideale B, se il primo ideale A è tutto contenuto nel secondo B.</u>

Dall'una o dall'altra definizione si ricavano subito le conseguenze elementari seguenti:

1) <u>Se l'ideale A è divisibile per B e questo per C, è anche A divisibile per C.</u>

Difatti A è contenuto in B, B in C e quindi A in C.

2) Ogni ideale A è divisibile per l'ideale unità O (perchè è contenuto in O).

3) L'ideale unità O è divisibile soltanto per sè stesso (come l'ideale più ampio).

4) Ogni ideale A ammette almeno due divisori, e cioè sè stesso e l'ideale unità.

Dopo ciò poniamo la definizione:

β) Un ideale A, diverso dall'ideale unità, che sia divisibile soltanto per sè stesso e per l'ideale unità, dicesi un ideale primo.

Vedremo fra breve che tali ideali primi esistono effettivamente e sono in numero infinito, essi saranno indicati con P; e conviene ricordare che (per definizione) l'ideale unità non si considera come ideale primo.

In secondo luogo, poniamo l'altra definizione:

γ) Due ideali A, B diconsi primi fra loro se non ammettono alcun divisore comune all'infuori dell'ideale unità.

Ne segue subito che:

Se P è un ideale primo, e A un altro qualunque ideale,

o A è primo con P, ovvero è divisibile per P. E infatti un divisor comune di A, P, come divisore di P, non può essere che P stesso, ovvero l'ideale unità.

Per proseguire nella esposizione della teoria della divisibilità degli ideali, conviene ora premettere qualche lemma sussidiario. In primo luogo dimostriamo:

A) Qualunque ideale A contiene infiniti numeri razionali interi, tutti multipli del minimo di essi.

Che in A esistano intanto dei numeri razionali vediamo per es. dal considerare che se α è un numero qualunque di A la norma di α è un numero razionale intero $N\alpha$, divisibile per α, e quindi contenuto in A. Ora la totalità degli interi razionali in A è manifestamente un ideale nel campo razionale; essi sono quindi tutti multipli del minimo di essi (cfr. § 7).

Stabiliamo ora quest'altra proposizione:

B) Un numero razionale intero positivo a appartiene soltanto ad un numero finito di ideali.

Se $a = 1$, ciò è evidente, perchè vi ha un solo ideale contenente 1, e cioè l'ideale unità. Supposto $a > 1$,

tutti gli interi di $K(\theta)$ si distribuiscono (mod (a)) in un numero finito di classi, precisamente (§ 24) in $Na = a^n$ classi, e siano

$$\beta_1, \beta_2, \cdots \beta_{Na}$$

un sistema completo di numeri (interi) di $K(\theta)$ incongrui mod a; ogni altro intero α si potrà porre sotto la forma

$$\alpha = \rho a + \beta_i .$$

Se l'ideale A contiene il numero a, potremo scrivere p.e.

$$A = (\alpha_1, \alpha_2, \cdots \alpha_\varrho, a),$$

e riducendo ciascun numero α_i (mod a), secondo la formola precedente, avremo

$$A = (\beta_1, \beta_2, \cdots \beta_\varrho, a),$$

dove le β eguali si possono scrivere una volta sola e tralasciare quelle nulle (cfr. § 23). Così, essendo a fisso, e finito il numero delle β, abbiamo soltanto un numero finito di possibili ideali A a cui a appartiene.

Dopo ciò siamo in grado di dimostrare l'altra proposizione:

C) Un ideale A ammette soltanto un numero finito di ideali C divisori.

Secondo il teorema fondamentale A) § 25, si determini un secondo ideale B tale che si abbia

$$AB = (a),$$

essendo a un numero razionale intero (positivo). Un divisore C di A divide anche il prodotto AB, ossia (a), vale a dire il numero razionale intero a appartiene a C, onde pel teorema B), il numero dei possibili C è finito.

Osserviamo ora che se l'ideale A è divisibile per $B \neq A$, il numero dei suoi divisori, sarà maggiore di quello dei divisori di B, perchè A è certamente divisibile per tutti i divisori di B e inoltre per A che non divide B, altrimenti sarebbe $A = B$. Di qui deduciamo facilmente l'altro teorema:

D) <u>Ogni ideale A diverso da 0 (dall'ideale unità) ammette almeno un divisore primo P.</u>

Fra tutti i divisori di A, diversi da 0, sia C quello che ha il minimo numero possibile di divisori; dico che C è primo. E infatti un suo divisore, diverso da C e da 0, dividerebbe anche A, ed avrebbe meno divisori di C.

Così dunque qualunque ideale A o è primo, o ammette un ideale primo P per divisore. Nel secondo caso poniamo

$$A = PA',$$

e proseguendo su A' nel medesimo modo (ove A' non sia già primo), e così di seguito, perverremo dopo un numero finito di operazioni (a causa del teorema C) al risultato:

E) Qualunque ideale A è risolubile nel prodotto di ideali primi

$$A = PP'P'' \dots P^{(r)} \qquad \text{(in numero finito)}.$$

I teoremi C), D), E) fin qui stabiliti offrono un'evidente analogia con teoremi corrispondenti dell'aritmetica razionale, ove all'ente ideale si sostituisca quello di numero intero razionale. Ma perchè l'analogia risulti completa manca ancora che dimostriamo il seguente:

F) Se un ideale primo P divide il prodotto AB di due ideali divide almeno uno di essi.

Supponiamo che P non divida A, e dimostriamo che, se divide AB, dividerà necessariamente B. Pongasi

$$A = (\alpha_1, \alpha_2, \dots \alpha_q) \quad , \quad P = (\pi_1, \pi_2, \dots \pi_s),$$

e riunendo i loro numeri generatori α_t, π_k si costruisca l'ideale

$$C = (\alpha_1, \alpha_2, \dots \alpha_q, \pi_1, \pi_2, \dots \pi_s),$$ [il massimo comun divisore di A, P secondo il § seguente],

nel quale tanto A quanto P sono contenuti, e però P è divisibile per C.

Siccome P è primo, o avremo $C = P$, o sarà C l'ideale unità. Ma la prima cosa porterebbe che ciascun numero α_i $(i = 1, 2, \dots q)$ apparterrebbe a P, e allora A stesso sarebbe contenuto in P, indi divisibile per P contro la ipotesi. Si ha perciò necessariamente $C = 0$, sicchè fra i numeri di C vi è anche 1, ed esistono in conseguenza dei moltiplicatori λ, μ interi in $K(\theta)$, tali che si abbia

$$\sum_{i=1}^{i=q} \lambda_i \alpha_i + \sum_{j}^{j=s} \mu_j \pi_j = 1$$

La prima somma dà un numero α di A, la seconda un numero π di P, tali che

$$\alpha + \pi = 1.$$

Prendasi allora un <u>qualunque</u> numero β di B, che si potrà scrivere per la precedente

$$\beta = \alpha\beta + \pi\beta.$$

Ora per ipotesi AB è divisibile per P cioè qualunque numero di AB trovasi in P, in particolare $\alpha\beta$ è contenuto in AB (§ 25) indi in P.

Ma anche $\pi\beta$ è contenuto in P, e per ciò anche $\beta = \alpha\beta + \pi\beta$. Così, qualunque numero β di B essendo contenuto in P, l'ideale B è divisibile per P c. d. d.

Da questo teorema discendono immediatamente i corollarii.

1) Se un ideale primo P divide il prodotto di più ideali, divide almeno uno dei fattori.

2) Se un ideale primo P divide il prodotto di più ideali primi, è uguale ad almeno uno di questi.

Ed ora, se supponiamo che un ideale A, applicando la decomposizione del teorema E), siasi risoluto in due modi nel prodotto di ideali primi P, Q

$$P_1 P_2 \ldots P_m = Q_1 Q_2 \ldots Q_{m'},$$

ne concludiamo che ciascun ideale P_i a sinistra trova il suo eguale Q_k a destra, dopo di che, sopprimendo questo fattore comune, come è lecito pel teorema al § 25, e proseguendo nel medesimo modo,

arriviamo al teorema principale della teoria:

Teorema principale. - Ogni ideale A, diverso dall'ideale unità 0, si risolve in un modo essenzialmente unico, nel prodotto di ideali primi (ove si prescinda dall'ordine dei fattori).

Naturalmente, in questa decomposizione dell'ideale A in fattori primi (ideali), un medesimo ideale primo potrà presentarsi più volte, e riunendo questi fattori eguali, si darà alla decomposizione la forma determinata

$$A = P_1^{n_1} P_2^{n_2} \ldots P_r^{n_r},$$

dove con $P_1, P_2, \ldots P_r$ indichiamo gli ideali primi diversi che entrano in A, e con $n_1\ n_2 \ldots n_r$ i rispettivi gradi (numeri interi positivi) a cui vi figurano.

§ 27

Massimo comun divisore - Minimo multiplo comune - Infinità degli ideali primi.

Nei teoremi fondamentali dimostrati nei paragrafi precedenti, l'aritmetica degli ideali nei corpi algebrici presenta una perfetta analogia coll'ordinaria arit-

metica razionale; gli ideali primi nell'aritmetica generale sono gli elementi coi quali si compongono tutti gli altri ideali, e funzionano dunque come i numeri primi nell'aritmetica razionale. E in questo ~~altro~~ campo, come in tutti gli altri ove coincidono le nozioni di numero indecomponibile e di numero primo, basta sostituire ai numeri gli ideali (principali) corrispondenti, per ricondurre questi casi particolari sotto le leggi generali.

E qui, proseguendo nella deduzione dei teoremi più rilevanti nella teoria degli ideali, osserviamo in primo luogo che, supposti risoluti gli ideali nei loro fattori primi, ne risulta subito come dalla decomposizione dei singoli fattori di un prodotto si ottiene la decomposizione del prodotto riunendo i fattori primi dei singoli fattori.

Precisamente come nell'aritmetica razionale, ne seguono allora le proposizioni:

a) <u>Se A e B sono due ideali, la condizione necessaria e sufficiente perchè A sia divisibile per B è che ciascun ideale primo P, fattore di B, entri in A</u>

<u>alla medesima potenza, o a potenza maggiore.</u>

b) <u>Se un ideale divide il prodotto di due ideali ed è primo con uno di questi, divide l'altro.</u>

c) <u>Se un ideale è divisibile per altri due primi fra loro, è divisibile pel loro prodotto.</u>

Dati due ideali A, B, si può stabilire la nozione dell'ideale loro <u>massimo comun divisore</u> (M.C.D) e quella dell'ideale loro <u>minimo multiplo comune</u> (m.c.m.) come segue.

Il primo si definirà come quel divisore comune D di A, B che ha la minima estensione possibile in numeri, e del quale quindi ogni altro divisor comune di A, B è necessariamente divisore. Note le decomposizioni di A, B in fattori primi, si ottiene subito quella di D nel quale figureranno tutti e soli i fattori primi comuni ad A e B, ciascuno elevato alla <u>minima</u> delle due potenze a cui vi figura. Ma è egualmente facile (dalla definizione) formare D, quando A e B siano definiti soltanto mediante rispettivi loro numeri generatori, diciamo

$$A = (\alpha_1, \alpha_2, \dots \alpha_q), \qquad B = (\beta_1, \beta_2, \dots \beta_s).$$

Siccome tanto A quanto B sono divisibili per D, saranno ambedue contenuti in D (§ 25 a)), e dovendo D avere

il minimo contenuto in numeri, sarà manifestamente

$$D = (\alpha_1, \alpha_2, \dots \alpha_q, \beta_1, \beta_2, \dots \beta_s).$$

In sostanza D è formato da tutte le somme di ogni numero di A con ogni numero di B. Quando $D = 0$ i due ideali sono primi, secondo la definizione μ) §26.

Definiremo poi il minimo multiplo comune di A, B come quell'ideale M che, essendo multiplo tanto di A quanto di B, ha la massima estensione possibile in numeri, ed è quindi divisore di ogni altro multiplo comune di A, B. Esso consta di tutti e soli i numeri comuni ad A e B. Dalla decomposizione di A, B in fattori primi si ottiene subito quella di M, i cui fattori primi sono quelli che compariscono o in A o in B (o in tutti due), ciascuno elevato alla massima delle due potenze a cui vi figura. Di qui risulta subito, come nell'aritmetica ordinaria

$$M = \frac{AB}{D},$$

e se A, B sono primi fra loro ($D = 1$), il minimo multiplo comune è il loro prodotto.

Naturalmente queste formazioni del (M. C. D) o del (m. c. m) si applicano anche ai numeri interi α, β

del corpo che vanno per ciò sostituiti dai corrispondenti ideali principali (α), (β) e ben s'intende che, in generale, non saranno nè D nè M alla loro volta principali.

La nozione di massimo comun divisore D e di minimo multiplo comune M si estende, nel medesimo modo, a quanti si vogliano ideali

$$A_1, A_2, \dots A_r,$$

e sarà D l'ideale che è composto di tutte le somme

$$\alpha_1 + \alpha_2 + \dots + \alpha_r,$$

percorrendo α_1 i numeri di A_1, α_2 quelli di A_2 ... ecc.; medesimamente M sarà l'ideale composto di tutti e soli i numeri comuni ad $A_1, A_2, \dots A_r$ (fra i quali figurano sempre i prodotti $\alpha_1 \alpha_2 \dots \alpha_r$). Gli r ideali A_1, $A_2, \dots A_r$ si dicono primi fra loro se il loro massimo comun divisore è l'ideale unità O, e in questo caso il numero $\underline{1}$, appartenente ad O, può porsi sotto la forma

$$\alpha_1 + \alpha_2 + \dots + \alpha_r = 1;$$

viceversa, se questo è possibile, gli r ideali sono primi fra loro (perchè D, contenendo $\underline{1}$ è l'ideale unità). Questo si può applicare in particolare al caso che A_1, A_2,

...A_r siano ideali principali $(\beta_1), (\beta_2), \dots (\beta_r)$, e ne segue: se gli r numeri $\beta_1, \beta_2, \dots \beta_r$ sono primi fra loro, si può sempre risolvere, in numeri interi $x_1, x_2, \dots x_r$ del corpo, l'equazione

$$\beta_1 x_1 + \beta_2 x_2 + \dots + \beta_r x_r = 1.$$

Consideriamo ora il caso di un ideale primo P, e sia p il più piccolo numero razionale intero positivo contenuto in P, secondo il teorema A) § 26. È facile vedere che p è necessariamente primo, perchè se consentisse un'effettiva decomposizione $p = q r$, indi $(p) = (q)(r)$, l'ideale primo P, dividendo il prodotto $(q)\cdot(r)$, dividerebbe uno almeno dei fattori, poniamo (q), ed allora il numero q, più piccolo di p, sarebbe contenuto in P. Così, ad ogni ideale primo P è coordinato uno ed uno solo numero primo ordinario p, che è il più piccolo razionale intero di P: Ogni ideale primo P divide uno ed un solo numero primo ordinario p. - Per costruire adunque nel corpo algebrico $K(\theta)$ la serie degli ideali primi basta saper risolvere nei loro ideali primi i numeri primi p ordinarii. E poichè la serie di questi ultimi è illimitata (Euclide), se ne con-

chiude la proposizione analoga dell'aritmetica generale dei corpi algebrici

In ogni corpo algebrico esistono infiniti ideali primi

§ 28

Congruenze simultanee di numeri rispetto ad ideali. Applicazioni.

Siano $A_1, A_2, \cdots A_r$ r ideali, i quali siano primi fra loro due a due, e quindi anche tutti fra loro. Come nella aritmetica ordinaria, e nelle sue prime estensioni (cfr. § 3 pel campo di Gauss), vale allora la proposizione fondamentale seguente:

A) Dati r interi qualunque $\alpha_1, \alpha_2, \cdots \alpha_r$, esiste un intero x che soddisfa alle congruenze simultanee

(1) $$x \equiv \alpha_1 \pmod{A_1}, \quad x \equiv \alpha_2 \pmod{A_2}, \ldots \; x \equiv \alpha_r \pmod{A_r},$$

e questo numero x è perfettamente determinato rispetto all'ideale $A_1 A_2, \ldots A_r$ prodotto di tutti gli ideali (loro minimo multiplo comune).

Poniamo

$$A = A_1 A_2 \cdots A_r \quad , B_1 = A_2 \cdots A_r = \frac{A}{A_1} \; , B_2 = A_1 A_3 \cdots A_r = \frac{A}{A_2}, \cdots B_r = A_1 \cdots A_{r-1} = \frac{A}{A_r};$$

gli ideali $B_1, B_2, \cdots B_r$ sono (complessivamente) primi fra

loro, perchè, se un ideale primo P li dividesse tutti, dovrebbe dividere uno degli A_i, poniamo A_1, e allora non può dividere $B_1 = A_2 A_3 \cdots A_r$, che è primo con A_1. Si può dunque estrarre un numero β_1 da B_1, uno β_2 da $B_2 \ldots$ uno β_r da B_r, tali che si abbia

$$(2) \qquad \beta_1 + \beta_2 + \cdots + \beta_r \equiv 1 ;$$

e allora poniamo

$$(3) \qquad x = \beta_1 \alpha_1 + \beta_2 \alpha_2 + \cdots + \beta_r \alpha_r ,$$

questo numero x soddisfa a tutte le congruenze (1). In ragione della simmetria delle formole, basterà provare per es. che soddisfa alla prima. Ora $\beta_2, \beta_3, \ldots \beta_n$ sono numeri dei rispettivi ideali $B_2, B_3 \cdots B_n$, tutti divisibili per A_1, e sono quindi tutti contenuti in A_1, ossia

$$\beta_2 \equiv \beta_3 \equiv \cdots \equiv \beta_n \equiv 0 \qquad (\text{mod } A_1) ,$$

dopo di che la (2) ci dà

$$\beta_1 \equiv 1 \ (\text{mod } A_1) ,$$

indi la (3) $x \equiv \alpha_1 \ (\text{mod } A_1)$ c. d. d. Se ora supponiamo che un secondo numero y soddisfi alle medesime congruenze, avremo

$$x - y \equiv 0 \ (\text{mod } A_1) \ , \quad x - y \equiv 0 \ (\text{mod } A_2) , \ \ldots \ x - y \equiv 0 \ (\text{mod } A_r),$$

e la differenza $x - y$, essendo divisibile per $A_1, A_2, \ldots A_r$, pri-

mi fra loro due a due, sarà divisibile anche per il loro prodotto $A = A_1 A_2 \cdots A_r$, ciò che completa la proposizione enunciata.

Risulta subito di qui che, se nella formola (3) si fa percorrere ad α_i un sistema completo di $N(A_i)$ numeri incongrui (mod A_i) per $i = 1, 2, \ldots r$, il numero $\underline{\alpha}$ percorrerà un sistema completo di numeri incongrui (mod $(A_1 A_2 \cdots A_r)$); si ha quindi

$$N(A_1 A_2 \cdots A_r) = N(A_1) \cdot N(A_2) \cdots N(A_r) .$$

Questo teorema (della norma del prodotto), qui dimostrato nel caso di fattori primi fra loro due a due, vale, come fra breve vedremo, affatto in generale (§ seguente).

Dalla proposizione A) stabilita possiamo dedurre una prima importante conseguenza contenuta nel teorema:

B) <u>Se l'ideale A è divisibile per l'ideale B, si può sempre trovare in B un numero η tale che i due ideali quozienti $\frac{A}{B}$, $\frac{(\eta)}{B}$ siano primi fra loro, cioè B sia il massimo comun divisore di A e di (η).</u>

Risolviamo B in fattori (ideali) primi, e sia

$$B = P_1^{n_1} P_2^{n_2} \cdots P_r^{n_r} ;$$

ciascuno P_i entra, per ipotesi, in A almeno alla medesima potenza n_i, e può inoltre A contenere altri ideali primi diversi, diciamo $Q_1, Q_2, \dots Q_s$. Prendiamo un numero α_i contenuto in $P_i^{n_i}$ ma non in $P_i^{n_i+1}$, come è sempre possibile, essendo $P_i^{n_i}$ più ampio in contenuto di $P_i^{n_i+1}$, e determiniamo, secondo A), un numero η che soddisfi alle congruenze simultanee

$$\begin{cases} \eta \equiv \alpha_1 \pmod{P_1^{n_1+1}}, \quad \dots \quad \eta \equiv \alpha_r \pmod{P_r^{n_r+1}} \\ \eta \equiv 1 \pmod{Q_1}, \quad \dots \quad \eta \equiv 1 \pmod{Q_s}, \end{cases}$$

le quali sono compatibili perchè i moduli sono primi fra loro due a due. Siccome $\alpha_i \equiv 0 \pmod{P_i^{n_i}}$, ma invece $\alpha_i \not\equiv 0 \pmod{P_i^{n_i+1}}$ il numero η è divisibile per $P_i^{n_i}$ ma non per $P_i^{n_i+1}$; e siccome $\eta \equiv 1 \pmod{Q_i}$ non è divisibile per alcuno degli ideali Q. Dunque η è divisibile per B, ma non contenendo alcun fattore P_i a potenza superiore di quella n_i a cui figura in B, e nessun altro dei fattori residui Q di A, il massimo comun divisore di A e di (η) è appunto B, come si voleva.

Possiamo ora ritornare sul risultato fondamentale del § 25, relativo alla conversione di ogni ideale

in un ideale principale per moltiplicazione con un altro ideale, e dimostrare

C) Un ideale qualunque B si può convertire in un ideale principale, moltiplicandolo per un conveniente ideale J che sia primo con un ideale prefissato arbitrario C.

Pongasi infatti nel precedente teorema B) l'ideale $A = BC$ e pel numero η ivi determinato si risolva l'ideale principale (η) in $(\eta) = BJ$. Allora appunto $J = \frac{(\eta)}{B}$, essendo primo con $C = \frac{A}{B}$, soddisfa alla condizione richiesta.

Un'altra conseguenza importante si trae dal teorema B), prendendo per A un ideale principale qualunque (α) divisibile per B, dove dunque α è un numero arbitrario di B. Ne segue l'esistenza di un altro numero $\beta = \eta$ in B, tale che B sia il massimo comun divisore di (α), (β), cioè dei numeri α, β. Troviamo così il notevole teorema

D) Qualunque ideale B può considerarsi come il massimo comun divisore di due convenienti suoi numeri α, β, dei quali uno può essere preso ad arbitrio.

Così dunque, mentre gli ideali principali sono ge-

nerabili con un solo numero $\underline{\alpha}$ tutti gli altri (secondarii) $\mathcal{J}$ possono generarsi con due numeri α, β, e si può scrivere nella notazione del § 23

$$\mathcal{J} = (\alpha, \beta),$$

cioè tutti i numeri di $\mathcal{J}$ si scrivono sotto la forma <u>binaria</u>

$$\alpha x_1 + \beta x_2$$

percorrendo x_1, x_2 tutti gli interi di $K(\theta)$. In sostanza adunque mentre nell'aritmetica razionale, ed in ogni altra in cui esistano soli ideali principali se $\alpha_1, \alpha_2, \dots \alpha_r$ sono interi fissi di $K(\theta)$ e $x_1, x_2, \dots x_r$ interi variabili, tutti i numeri della forma

$$\alpha_1 x_1 + \alpha_2 x_2 + \dots \alpha_r x_r ,$$

costituenti l'ideale $(\alpha_1, \alpha_2, \dots \alpha_r)$, sono riducibili alla forma ρx, nell'aritmetica generale dei corpi algebrici sono riconducibili alla forma binaria

$$\beta_1 y_1 + \beta_2 y_2 ,$$

dove β_1, β_2 sono interi fissi, soddisfacenti alla sola condizione di avere l'ideale $(\alpha_1, \alpha_2, \dots \alpha_r)$ quale massimo comun divisore.

Il teorema della norma del prodotto - Grado degli ideali primi.

Dalle considerazioni precedenti si può anche trarre la dimostrazione di un importante teorema, già sopra dimostrato per un caso particolare, e che si enuncia:

A) La norma di un prodotto di quanti si vogliano ideali è uguale al prodotto delle loro norme.

Basterà manifestamente dimostrarlo nel caso di due fattori B, C qualunque collo stabilire la formula

$$N(BC) = N(B) \cdot N(C) . \tag{1}$$

Secondo il teorema C) del § precedente, possiamo scegliere un ideale A primo con C, tale che

$$AB = (\eta)$$

risulti un ideale principale generato dal numero η, che sarà $\equiv 0 \pmod{B}$. Posto $N(B) = b$, $N(C) = c$ indichiamo con

$$\xi_1, \xi_2, \cdots \xi_b$$

un sistema (completo) di b numeri incongrui (mod B), e con

$$\beta_1, \beta_2, \cdots \beta_c$$

un sistema (completo) di c numeri incongrui (mod C).
Consideriamo allora i bc numeri

$$(2) \qquad \eta\beta_i + \xi_k \qquad \begin{cases} i = 1, 2, \cdots c \\ k = 1, 2, \cdots b \end{cases}$$

e dimostriamo che sono tutti incongrui (mod BC), mentre ogni altro numero ω di $K(\theta)$ è congruo con uno dei (2); così sarà appunto provata la (1).

1°- Due numeri diversi (2) sono incongrui (mod BC).

Supponiamo

$$(3) \qquad \eta\beta_i + \xi_k \equiv \eta\beta_j + \xi_l \quad (\text{mod } BC);$$

siccome $\eta \equiv 0$ (mod B), ne dedurremo

$$\xi_k \equiv \xi_l \quad (\text{mod } B),$$

indi necessariamente $k = l$, $\xi_k = \xi_l$. Dopo ciò la (3) resta

$$\eta(\beta_i - \beta_j) \equiv 0 \quad (\text{mod } BC)$$

e dice che il prodotto dell'ideale principale $(\eta) = AB$ per l'altro principale $(\beta_i - \beta_j)$ è divisibile per BC, onde segue che il prodotto di A per $(\beta_i - \beta_j)$ è divisibile per C. Ma C è primo con A e dividendo il prodotto

$$A \cdot (\beta_i - \beta_j)$$

divide in conseguenza $(\beta_i - \beta_j)$, ossia

$$\beta_i \equiv \beta_j \pmod{C},$$

ciò che è assurdo se non è $\beta_i = \beta_j$.

2°.- Ogni numero ω di $K(\theta)$ è congruo con uno dei numeri (2) (mod BC).

Intanto sarà ω certamente (mod B) congruo con uno dei numeri ξ, poniamo con ξ_k, e facciamo

$$(4) \qquad \omega - \xi_k = \beta, \text{ con } \beta \equiv 0 \pmod{B}.$$

Siccome A è primo con C esisterà un numero α in A e un numero ρ in C tali che sia

$$1 = \alpha + \rho,$$

indi

$$\beta = \beta\alpha + \beta\rho.$$

Ma β è divisibile per B, e ρ per C, onde $\beta\rho$ è divisibile per BC, e dalla precedente risulta

$$(5) \qquad \beta \equiv \beta\alpha \pmod{BC}.$$

Essendo poi α divisibile per A (β per B) è $\beta\alpha$ divisibile per $AB = (\eta)$, vale a dire multiplo di η, poniamo

$$\beta\alpha = \eta\nu.$$

Questo numero ν sarà congruo (mod C) con un numero β_i, cioè $\nu - \beta_i$ sarà divisibile per C, e siccome η lo è per B, sarà $\eta(\nu - \beta_i)$ divisibile per BC, cioè $\eta\nu \equiv \eta\beta_i \pmod{BC}$, indi

$$\beta\alpha \equiv \eta\beta_i \pmod{BC}.$$

Dalla (5) segue dunque

$$\beta \equiv \eta\beta_i \pmod{BC}$$

e per ciò dalla (4) considerata rispetto al modulo BC

$$\omega \equiv \eta\beta_i + \xi_k ,$$

che è quanto volevasi provare.

- Del teorema generale A) dimostrato si osservi il caso particolare che uno dei due ideali per es. B sia principale (β); allora avremo

$$N((\beta)\cdot C) = |N\beta|\cdot N(C).$$

Questo risulta anche direttamente dalla relazione della norma di un ideale col discriminante della base (§ 24), poichè se $[\gamma_1, \gamma_2, \cdots \gamma_n]$ è una base di C, manifestamente è $[\beta\gamma_1, \beta\gamma_2, \cdots \beta\gamma_n]$ una base di $(\beta)\cdot C$, e d'altronde si trova subito

$$\Delta(\beta\gamma_1, \beta\gamma_2, \cdots \beta\gamma_n) = |N\beta|^2\cdot \Delta(\gamma_1, \gamma_2, \cdots \gamma_n).$$

Sulle norme degli ideali notiamo anche questo semplice teorema:

B) <u>Fra i numeri razionali contenuti in qualunque ideale A figura sempre il numero dato dalla norma dell'ideale: $N(A) \equiv 0 \pmod{A}$.</u>

Se poniamo infatti $\mathcal{N}(A) = a$ e consideriamo un sistema completo di $\underline{a}$ numeri incongrui (mod A)

$$\alpha_1\ ,\ \alpha_2\ ,\ \cdots\ \alpha_a\ ,$$

anche

$$1+\alpha_1\ ,\ 1+\alpha_2\ ,\ \cdots\ 1+\alpha_a$$

formano un tale sistema completo, e le somme dei numeri in ciascun sistema sono dunque congrue (mod A):

$$\alpha_1 + \alpha_2 + \cdots + \alpha_a \equiv a + \alpha_1 + \alpha_2 + \cdots \alpha_a \pmod{A},$$

ossia

$$a = \mathcal{N}(A) \equiv 0 \pmod{A} \quad \text{c.d.d.}$$

Ricordando ora la proposizione stabilita in B) § 26, ne deduciamo questa conseguenza:

C) <u>Per ogni ideale A del corpo $K(\theta)$ esiste soltanto un numero finito di altri ideali che abbiano la stessa norma.</u>

Così per es. esiste un solo ideale di norma $= 1$ ed è l'ideale unità. E si osservi che, se ci limitassimo a considerare ideali principali, due tali ideali di egual norma sono necessariamente identici, i loro numeri generatori essendo associati.

Consideriamo da ultimo il caso di un ideale primo P, e sia $\underline{p}$ il numero primo ordinario coordinato a P secondo il § 27. Siccome P divide p, così $\mathcal{N}(P)$ dividerà $\mathcal{N}(p)$ (pel teorema A)); ma d'altra parte indicando $\underline{n}$ il grado del corpo è

$$\mathcal{N}(p) = p^n,$$

indi necessariamente

$$\mathcal{N}(P) = p^f$$

con f intero (positivo) non superiore a $\underline{n}$. Dunque:

La norma di un ideale primo P è sempre una potenza esatta p^f del numero primo p coordinato all'ideale.

Questo esponente f, che in ogni caso non eccede il grado $\underline{n}$ del corpo, dicesi il grado dell'ideale primo P.

Si osserverà che, ove il numero primo $\underline{p}$ si risolva in $K(\theta)$ nei suoi fattori ideali primi diversi $P_1, P_2, \dots P_r$, se si ha

$$p = P_1^{e_1} P_2^{e_2} \dots P_r^{e_r},$$

e si indicano con $f_1, f_2, \dots f_r$ i rispettivi gradi di $P_1, P_2, \dots \dots P_n$ (ai quali tutti è coordinato il numero primo p), prendendo le norme a sinistra e a destra risulta pel teorema A)

$$n = e_1 f_1 + e_2 f_2 + \cdots + e_r f_r .$$

In ogni caso adunque $r \leq n$; e se $r = n$, allora tutti i fattori $P_1, P_2, \ldots P_n$ sono di 1° grado, e il numero p è il loro prodotto.

Dal teorema A) delle norme segue ancora il corollario: se le norme di due ideali A, B sono numeri primi fra loro anche gli ideali A, B sono primi fra loro, altrimenti la norma del loro divisore comune dividerebbe insieme NA, NB. Il teorema non è manifestamente invertibile.

§ 30

La funzione $\Phi(A)$ generalizzata e il teorema di Fermat - Resti di potenze

Le considerazioni svolte al principio del § precedente possono anche applicarsi a rispondere alla domanda: Dato un ideale qualunque A, quanti sono fra gli $N(A)$ numeri incongrui (mod A) quelli che sono primi coll'ideale stesso?

[Si noti che due numeri congrui (mod A) sono sempre insieme primi, ovvero non primi con A].

Questo numero, che si indica con $\Phi(A)$, è manifestamente la generalizzazione della funzione numerica $\varphi(m)$ di Gauss dell'aritmetica razionale. Secondo quanto si è visto sopra, essendo B, C due ideali qualunque, gli $N(BC)$ numeri dati dalla serie (2) formano un sistema completo di numeri incongrui (mod BC) e per risolvere la questione proposta noi risolviamo prima la seguente: <u>Quanti sono fra gli $N(BC)$ numeri (2) quelli non divisibili per B?</u> Siccome nella (2) η è divisibile per B, i numeri della serie (2) <u>divisibili</u> per B sono tutti e soli quelli in cui $\xi \equiv 0 \pmod B$, vale a dire sono in numero di $N(C)$. Togliendoli dalla serie (2), restano precisamente $N(BC) - N(C) = N(C)(N(B)-1)$ numeri che sono quelli domandati (non divisibili per B).

In questo risultato, indicando con P un ideale primo, e con r un intero positivo qualunque, poniamo

$$B = P \quad , \quad C = P^{r-1}$$

ed avremo che, fra gli $N(P^r)$ numeri incongrui (mod P^r), di non divisibili per P, cioè a dire primi con P, indi con P^r, ne esiste un numero dato da

$$(NP)^{r-1}(NP-1) ;$$

si ha dunque:

$$(1) \qquad \Phi(P^r) = (NP)^{r-1}(NP-1) = (NP)^r\left(1-\frac{1}{NP}\right).$$

Così è trovata la funzione $\Phi(A)$ nel caso che A sia una potenza di un ideale primo. Per trovarla in generale, serviamoci di quest'altro teorema:

<u>Se $A_1, A_2, \dots A_r$ sono ideali primi fra loro due a due, si ha</u>

$$(2) \qquad \Phi(A_1 A_2 \dots A_r) = \Phi(A_1)\cdot\Phi(A_2)\cdots\Phi(A_r).$$

Questo deriva facilmente dalle osservazioni al principio del § 28, in modo analogo come dalla formola (3) ibid. abbiamo tratto $N(A_1 A_2 \dots A_r) = N(A_1)\cdot N(A_2)\dots N(A_r)$. Basta infatti osservare che il numero $\underline{x}$, dato da questa formola, riesce primo col prodotto $A_1 A_2 \dots A_r$ allora ed allora soltanto che β_1 sia primo con A_1, β_2 con $A_2 \dots$ β_r con A_r, onde la formola sopra scritta riesce evidente.

Dopo ciò prendiamo un ideale A qualunque, e risoluto in fattori primi diversi sia

$$A = P_1^{n_1} P_2^{n_2} \dots P_r^{n_r};$$

avremo per la (2)

$$\Phi(A) = \Phi(P_1^{n_1})\cdot\Phi(P_2^{n_2})\cdots\Phi(P_r^{n_r}),$$

ed applicando la (1)

$$\Phi(P_i^{a_i}) = (\mathcal{N}P_i)^{a_i}\left(1 - \frac{1}{\mathcal{N}P_i}\right),$$

onde sostituendo

$$(I) \qquad \Phi(A) = \mathcal{N}(A)\left(1 - \frac{1}{\mathcal{N}P_1}\right)\left(1 - \frac{1}{\mathcal{N}P_2}\right)\cdots\left(1 - \frac{1}{\mathcal{N}P_r}\right),$$

formola perfettamente analoga a quella per la $\varphi(m)$ in aritmetica razionale (cfr. anche § 3 formola (A) pei numeri di Gauss. Similmente si generalizza una nota proprietà della $\varphi(m)$ nell'altra

$$\sum \Phi(D) = \mathcal{N}(A),$$

dove s'intende che a sinistra D percorrerà tutti gli ideali divisori di A, compreso l'ideale unità O pel quale è da farsi $\Phi(O) = 1$.

Per generalizzare ora anche il teorema di Fermat (Eulero), premettiamo l'osservazione: <u>Se nel binomio $\alpha x + \beta$, dove α e β sono due interi fissi nel corpo, dei quali il primo α sia primo coll'ideale A, si fa percorrere a x un sistema completo di $N(A)$ numeri incongrui (mod A), anche $\alpha x + \beta$ percorre un tale sistema.</u>

E infatti da $\alpha x + \beta \equiv \alpha x' + \beta \pmod{A}$, segue $\alpha(x - x') \equiv 0 \pmod{A}$ e, <u>perchè α è primo con A</u>, ne risulta

$x \equiv x' \pmod{A}$.

Segue di qui: <u>Nel corpo algebrico $K(\vartheta)$ la congruenza lineare</u>

$$\alpha x + \beta \equiv 0 \pmod{A},$$

<u>quando α è primo con A, ammette sempre una ed una sola radice</u>.

Supponendo ora $\beta = 0$, nel binomio αx facciamo percorrere a x solo i $\Phi(A)$ valori primi con A, diciamo

$$\rho_1, \rho_2, \dots \rho_{\Phi(A)}$$

Allora anche i numeri

$$\alpha\rho_1, \alpha\rho_2 \dots \alpha\rho_{\Phi(A)}$$

saranno incongrui fra loro e primi con A, e perciò congrui in altro ordine coi precedenti. Eseguendo il loro prodotto e ponendo $\rho = \rho_1 \rho_2 \cdots \rho_{\Phi(A)}$, risulta

$$\rho\alpha^{\Phi(A)} \equiv \rho \pmod{A},$$

e quindi, essendo ρ primo con A

$$\text{(II)} \qquad \alpha^{\Phi(A)} \equiv 1 \pmod{A}.$$

Questa formola, nella quale A denota ideale qualunque e α un numero <u>primo</u> con A, ci dà manifestamente il <u>teorema di Fermat</u> generalizzato.

Dopo questi risultati, non vi è alcuna difficoltà

a generalizzare gli altri teoremi ben noti dell'aritmetica razionale, fra i quali ci interessano particolarmente quelli relativi ai resti di potenze; le deduzioni sono identiche a quelle già esposte al § 4 pel caso speciale del campo di Gauss $K(\sqrt{-1})$, e basterà indicarle sommariamente.

Se α è un numero primo coll'ideale A, nella serie illimitata di potenze di α

$$\alpha^0 = 1\ ,\ \alpha\ ,\ \alpha^2\ ,\ \alpha^3, \ldots$$

ve ne è una prima $\alpha^\delta \equiv 1 \pmod{A}$, e questo esponente razionale intero positivo $\underline{\delta}$ dicesi l'esponente $\underline{\delta}$ cui appartiene $\alpha \pmod{A}$. Per la congruenza di due potenze di $\alpha \pmod{A}$ è necessario e sufficiente che gli esponenti siano congrui $(\text{mod}\ \delta)$; ne segue: <u>δ è in ogni caso un divisore di $\Phi(A)$</u>. Valgono pure le proprietà raccolte sotto $\beta)$, $\gamma)$, $\delta)$ al § 4, pel caso dei numeri di Gauss, senza che qui ne ripetiamo l'enunciato.

§ 31

Caso di un modulo primo P. - Estensione della teoria degli indici. - Residui quadratici.

Supponiamo ora che il modulo P sia un ideale pri=

mo e consideriamo una congruenza di grado qualunque m in una incognita x

$$(1) \qquad f(x) = \alpha_0 x^m + \alpha_1 x^{m-1} + \dots + \alpha_{m-1} x + \alpha_m \equiv 0 \pmod P$$

dove $\alpha_0, \alpha_1 \dots \alpha_m$ sono interi fissi nel corpo $K(\theta)$, dei quali il primo α_0 deve supporsi non divisibile per P (o ciò che è lo stesso primo con P), altrimenti se $\alpha_0 \equiv 0 \pmod P$ la congruenza abbasserebbe di grado; cerchiamo se esistono valori interi $x = \beta$ (nel corpo $K(\theta)$) che soddisfino la (1), nel qual caso β si dirà una radice. La questione è di trovare, se esistono, le radici diverse cioè incongrue $(\text{mod } P)$. Per il caso del grado $m = 1$ sappiamo già che la congruenza ha una ed una sola radice. E di qui, col procedimento usuale, si deduce facilmente:

La congruenza (1) di grado m rispetto ad un ideale primo P non può avere più di m radici.

Basta per questo riprendere il ragionamento stesso esposto al § 3 pel caso del corpo $K(\sqrt{-1})$ ed osservare che, se la (1) avesse più di m radici, se ne dedurrebbe una di grado $m-1$ con più di $m-1$ radici, e così proseguendo si arriverebbe ad una congruenza di 1° grado con più di una radice, risultato assurdo. E, come al § 3,

si dimostra che se $f(x)$ è scindibile nel prodotto di due polinomii

$$f(x) = \varphi(x)\,\psi(x)$$

con coefficienti interi in $K(\theta)$, quando la $f(x) \equiv 0 \pmod P$ abbia tante radici quante unità nel grado, altrettanto accade di ciascuna delle due

$$\varphi(x) \equiv 0 \quad , \psi(x) \equiv 0 \pmod P.$$

Dopo ciò consideriamo i $\Phi(P) = NP-1$ numeri incongrui (mod P) e non divisibili per P; ciascuno di essi appartiene ad un esponente δ divisore di $\Phi(P)$ e fra tutti questi esponenti il massimo $\underline{d}$ è multiplo di tutti gli altri (v. § 3 δ)). Se $\underline{x}$ è uno qualunque degli $NP-1$ numeri incongrui (non divisibili per P) e δ l'esponente cui appartiene, si ha $x^\delta \equiv 1 \pmod P$, e quindi anche, perchè $\underline{d}$ è multiplo di δ,

$$x^d - 1 \equiv 0 \pmod P.$$

Questa congruenza ha dunque $\Phi(P)$ radici incongrue, e poichè il suo grado $\underline{d}$ è in ogni caso un divisore di $\Phi(P)$, risulta necessariamente dal teorema sopra dimostrato che si ha

$$d = \Phi(P) = N(P) - 1.$$

Per conseguenza esistono dei numeri ρ che appartengono all'esponente di Fermat $\Phi(P)$, e facilmente si vede che ne esistono precisamente $\Phi(\Phi(P)) = \Phi(NP-1)$; li diremo numeri <u>primitivi</u> o anche <u>radici primitive</u> (mod P). Prendiamo una qualunque di queste radici primitive ρ, e consideriamo le sue prime $\Phi(P)$ potenze

$$\rho^0 = 1, \rho, \rho^2, \dots \rho^{\Phi(P)-1}$$

le quali dànno $\Phi(P)$ numeri incongrui (mod P), non divisibili per P, e per ciò tutti i possibili. Se prendiamo dunque un qualunque intero ρ, non divisibile per P, fra gli esponenti $0, 1, 2, \dots \Phi(P)-1$ ne esiste uno ed uno soltanto diciamo <u>m</u> tale che si abbia

$$\rho^m \equiv \rho \; ;$$

allora <u>m</u> si dirà l'indice di ρ (in base ρ) e si scriverà:

$$m = \operatorname{ind}_\rho \rho .$$

Stabilite queste nozioni fondamentali, è chiaro come tutta la teoria degli indici dell'aritmetica razionale vale nello stesso modo nel caso generale, e nelle applicazioni: La congruenza di due numeri ρ, ρ' (mod P) equivale alla congruenza dei loro indici (mod $\Phi(P)$).

Così rispetto agli ideali primi P, nell'aritmetica generale, si possono costruire <u>tabelle d'indici</u> che servono precisamente agli stessi scopi come nell'aritmetica elementare. [Però nell'aritmetica generale non si sa ancora se questo può farsi anche per potenze P^m di un ideale primo P, se cioè esistano anche in questo caso, come nell'aritmetica elementare nel caso di un numero primo p dispari, radici primitive, vale a dire appartenenti all'esponente di Fermat $\Phi(P^m)$].

In primo luogo, costruita una tabella d'indici per l'ideale primo P, si possono immediatamente risolvere le congruenze lineari

$$\alpha x \equiv \beta \pmod{P} \quad (\alpha \text{ non divisibile per } P)$$

calcolando ind x da

$$\text{ind}\, x \equiv \text{ind}\, \beta - \text{ind}\, \alpha \pmod{\Phi(P)}.$$

Consideriamo ancora le congruenze binomie

$$(2) \qquad x^m \equiv D \pmod{P},$$

nella quale <u>m</u> è un intero positivo che può supporsi $\leq \Phi(P)$, e D un intero del corpo non divisibile per P. Se la (2) ammette radici, il numero D si dirà <u>residuo</u>

m^{mo} (mod. P) Prendendo gli indici, la (2) è perfettamente sostituibile dalla congruenza dell'aritmetica elementare

$$m \operatorname{ind} x \equiv \operatorname{ind} \mathcal{D} \pmod{\Phi(P)},$$

per cui indicando con δ il massimo comun divisore di m e $\Phi(P)$, sarà $\mathcal{D}$ residuo m^{mo} (mod P) quando sia

$$(3) \qquad \operatorname{ind} \mathcal{D} \equiv 0 \pmod{\delta}$$

e, soddisfatta questa condizione, la (2) possiede δ radici incongrue. La condizione (3), che qui appare dipendente dalla radice primitiva g scelta a base, si trasforma subito nell'altra

$$(4) \qquad \mathcal{D}^{\frac{\Phi(P)}{\delta}} \equiv 1 \pmod{P}.$$

Il numero dei residui m^{mi} (mod P) è dato quindi dal numero delle radici della congruenza binomia

$$x^{\frac{\Phi(P)}{\delta}} \equiv 1 \pmod{P} \qquad (\delta = \text{massimo comun divisore di } m, \Phi(P))$$

e poichè $x^{\Phi(P)} - 1$ è divisibile per $x^{\frac{\Phi(P)}{\delta}} - 1$ questo numero è precisamente $\frac{\Phi(P)}{\delta}$.

Particolarmente interessante è il caso $m = 2$ dei <u>residui quadratici</u>, ove si introdurrà il simbolo generalizzato di Legendre $\left[\frac{\mathcal{D}}{P}\right]$ a significare l'unità po-

sitiva se $\mathfrak{D}$ è residuo, ha negativa se $\mathfrak{D}$ è non residuo. Valgono manifestamente per questo simbolo le proprietà elementari espresse dalle formole

$$\left[\frac{\mathfrak{D}}{P}\right] = \left[\frac{\mathfrak{D}'}{P}\right], \quad \text{se} \quad \mathfrak{D} \equiv \mathfrak{D}' \pmod{P}$$

$$\left[\frac{\mathfrak{D}_1\mathfrak{D}_2\ldots\mathfrak{D}_r}{P}\right] = \left[\frac{\mathfrak{D}_1}{P}\right]\left[\frac{\mathfrak{D}_2}{P}\right]\cdots\left[\frac{\mathfrak{D}_r}{P}\right], \quad \text{se} \quad \mathfrak{D} = \mathfrak{D}_1\mathfrak{D}_2\ldots\mathfrak{D}_r.$$

Ora osserviamo che se p è il numero primo coordinato all'ideale P, ed f il grado di questo ideale (§ 29)

$$\mathcal{N}(P) = p^f, \quad \Phi(P) = p^f - 1$$

e perciò se $p = 2$ il numero $\Phi(P)$ è dispari e in tutti gli altri casi è pari. E siccome qui $m = 2$, si ha nel primo caso $\delta = 1$, nel secondo $\delta = 2$, onde applicando la (4) si vede che:

a) Se l'ideale primo P divide il numero 2 allora qualunque numero $\mathfrak{D}$ è suo residuo quadratico.

b) Se il numero primo p, coordinato all'ideale primo P, è dispari, allora $\mathfrak{D}$ è residuo quadratico (mod P) solo quando

$$(5) \qquad \mathfrak{D}^{\frac{1}{2}\Phi(P)} \equiv 1 \pmod{P}.$$

Ora in questo caso b) avendosi

$$\mathfrak{D}^{\Phi(P)} - 1 = \left(\mathfrak{D}^{\frac{1}{2}\Phi(P)} - 1\right)\left(\mathfrak{D}^{\frac{1}{2}\Phi(P)} + 1\right) \equiv 0 \pmod{P},$$

o il primo, o il secondo dei due fattori è divisibile

per P, ma non tutti e due perchè la loro differenza $\underline{2}$ non è per ipotesi divisibile per P. Si hanno dunque le formole perfettamente corrispondenti al criterio d'Eulero:

D è residuo quadratico o non residuo di un ideale primo P (non divisibile per 2) secondo che

$$D^{\frac{1}{2}\Phi(P)} \equiv 1 \pmod{P}, \quad \text{o} \quad D^{\frac{1}{2}\Phi(P)} \equiv -1 \pmod{P},$$

ossia col simbolo di Legendre

$$\left[\frac{D}{P}\right] \equiv D^{\frac{1}{2}\Phi(P)} \pmod{P}.$$

Senza ricorrere alla teoria degli indici, questi ultimi risultati si stabiliscono del resto elementarmente come segue (cfr. Dirichlet-Dedekind § 34). Siano

$$(6) \qquad \rho_1, \rho_2 \cdots \rho_{\Phi(P)}$$

i $\Phi(P)$ numeri incongrui (mod P) (non divisibile per P). Se dapprima P divide $\underline{2}$ (se 2 è il numero primo coordinato), allora i $\Phi(P)$ quadrati

$$\rho_1^2, \rho_2^2 \cdots \rho_{\Phi(P)}^2$$

sono tutti incongrui (mod P) e rappresentano quindi tutti i numeri possibili, onde risulta nuovamente la a). E infatti supposto

$$\rho_i^2 \equiv \rho_k^2 \pmod{P},$$

siccome P divide 2 è anche

$$(\rho_i - \rho_k)^2 = \rho_i^2 + \rho_k^2 - 2\rho_i\rho_k \equiv 2\rho_i^2 - 2\rho_i \cdot \rho_k \equiv 0 \pmod{P},$$

cioè $\rho_i \equiv \rho_k \pmod{P}$.

Se invece P non divide $\underline{2}$, allora due numeri opposti $\rho_i, -\rho_i$ sono sempre incongrui e dànno lo stesso quadrato, onde vi sono $\frac{1}{2}\Phi(P)$ residui quadratici, e altrettanti non residui.

Per ritrovare il criterio d'Eulero si associno i numeri (6) a coppie così che

$$\rho_i \rho_k \equiv D \pmod{P};$$

ogni numero determina il suo associato e coincide con esso nel solo caso che sia radice di $x^2 \equiv D \pmod{P}$. Se dunque D è non residuo i numeri (6) si distribuiscono in $\frac{1}{2}\Phi(P)$ coppie di numeri distinti e il prodotto dei numeri in ciascuna coppia è $\equiv D$; per ciò

$$\rho_1 \rho_2 \cdots \rho_{\Phi(P)} \equiv D^{\frac{1}{2}\Phi(P)} \quad \text{se} \quad \left[\frac{D}{P}\right] = -1$$

Nel caso invece che D sia residuo la $x^2 \equiv D \pmod{P}$ ha due radici incongrue $\rho, -\rho$ e il loro prodotto è $-\rho^2 \equiv -D \pmod{P}$; i rimanenti numeri (6) si ordinano in $\frac{1}{2}(\Phi(P)-1)$ coppie, e per ciò

$$\rho_1 \rho_2 \cdots \rho_{\Phi(P)} \equiv -D^{\frac{1}{2}\Phi(P)} \quad \text{se} \quad \left[\frac{D}{P}\right] = +1.$$

Siccome in ogni caso il numero $D=1$ è residuo, ne

segue in primo luogo il teorema (generalizzato) di Wilson

$$\rho_1 \rho_2 \cdots \rho_{\Phi(P)} \equiv -1 \pmod{P},$$

e di nuovo il criterio d'Eulero

$$\begin{cases} D^{\frac{1}{2}\Phi(P)} \equiv 1 & \text{se } \left[\frac{D}{P}\right] = +1 \\ \qquad\qquad \pmod{P} & \\ D^{\frac{1}{2}\Phi(P)} \equiv -1 & \text{se } \left[\frac{D}{P}\right] = -1 \end{cases}$$

§ 32

Determinazione degli ideali primi nei corpi quadratici.

Per applicare in un caso concreto le teorie generali esposte nei paragrafi precedenti, prendiamo l'esempio dei corpi quadratici ($n = 2$), già considerato al § 14, e proponiamoci in questo caso di eseguire l'effettiva ricerca degli ideali primi nel corpo $K(\theta)$. Ricordiamo dal § 14 che, essendo d un numero razionale intero privo di fattori quadrati, il numero fondamentale D del corpo è

$$D = 4d \qquad \text{se } d \equiv 2, 3 \pmod 4$$

$$D = d \qquad \text{se } d \equiv 1 \pmod 4,$$

ed in ogni caso si ha una base del corpo nei due numeri

$$\omega_1 = 1 \qquad \omega_2 = \theta = \frac{D+\sqrt{D}}{2}.$$

Ad ogni ideale primo P del corpo è coordinato un numero primo ordinario p, che può essere il 2, ovvero un numero dispari e il grado f dell'ideale può essere

$$f = 1 \qquad \text{con} \quad NP = p$$

$$f = 2 \qquad \text{con} \quad NP = p^2.$$

Nel primo caso l'ideale principale (p) sarà scindibile nel prodotto di due ideali P, P', ciascuno di 1° grado, che potranno essere distinti ovvero coincidenti; nel secondo caso l'ideale principale (p) sarà esso stesso un ideale primo P di secondo grado. In qualunque caso poi i p numeri

$$(1) \qquad 0, 1, 2, \ldots p-1$$

sono incongrui (mod P) perchè la differenza di due di essi, essendo $< p$, non può essere contenuta nell'ideale P. È ben naturale che, dato il numero primo p, la decisione fra i due casi, se cioè l'ideale principale (p) si risolva nel prodotto di due ideali P, P' (distinti o coincidenti), ovvero sia un ideale primo, dovrà dipendere dalla specie del numero primo p, ed in effetto si vedrà che avviene il primo od il secondo caso second[o]

che D è residuo quadratico ovvero non residuo di $4p$.

Suppongasi infatti il 1° caso

$$(p) = P.P'$$

e si osservi che, essendo qui $NP = p$, i p numeri razionali interi (1) formano già un sistema completo di numeri incongrui (mod P), e per ciò ve ne sarà uno fra questi congruo (mod P) col numero fondamentale θ del corpo, sia

$$s \equiv \theta \pmod{P},$$

dove sarà s razionale intero.

Il numero

$$(2) \qquad \pi = \theta - s = \frac{r + \sqrt{D}}{2}, \qquad \text{con} \quad r = D - 2s$$

è dunque divisibile per P, indi il suo coniugato è

$$(2') \qquad \pi' = \theta' - s = \frac{r - \sqrt{D}}{2}$$

e si ha per la norma

$$N(\pi) = \pi\,\pi' = \frac{r^2 - D}{4}.$$

Ma, essendo π divisibile per P, risulta che $N(\pi)$ sarà divisibile per $N(P) = p$, cioè $\frac{r^2 - D}{4p}$ è intero, ossia

$$(3) \qquad r^2 \equiv D \pmod{4p}.$$

In questo primo caso è dunque necessariamente D residuo quadratico di $4p$. Ma inversamente, se que-

sto accade, ed è r una radice di questa (3), si ha anche $r \equiv D \pmod 2$, onde il numero $s = \frac{D-r}{2}$ è intero (razionale) e, risolvendo alla (2) e (2'), si vede che questi numeri π, π' sono interi di $K(\theta)$ che non sono singolarmente divisibili per p, mentre lo è il loro prodotto $\pi\pi' = N(\pi)$. Dunque l'ideale (p), dividendo il prodotto $\pi\pi'$ senza dividere alcuno dei fattori, non è primo e per conseguenza

$$(4) \qquad (p) = PP'.$$

La proposizione enunciata è così dimostrata.

Possiamo ora domandare di più, nel caso che valga la (4) (D residuo di $4p$), se i due ideali P, P' sono distinti o coincidenti. Per questo osserviamo che in ogni caso, dei due numeri sopra costruiti π, π', il primo essendo divisibile per P ma non per p, il secondo π' lo è per P'. E infatti ponendo

$$(\pi) = PQ\,,$$

l'ideale Q non è divisibile per P' (perchè (π) non è divisibile per $p = PP'$); d'altronde $(\pi)(\pi') = PQ(\pi')$ è divisibile per $p = PP'$, per ciò $Q.(\pi')$ è divisibile per P', indi (Q essendo primo con P') sarà (π'), ossia π' divisibile per P', c.d.d.

Ciò posto, supponiamo che sia $P' = P$. In tal caso an-

bedue i numeri π, π' sono divisibili per P, per ciò anche la loro somma $\pi + \pi' = r$; ma poichè r è razionale, sarà r stesso divisibile pel numero primo p [p.e. da che $N(r) = r^2$ deve essere divisibile per $N(P) = p$], e allora dalla (3) segue che <u>p è un fattore del numero fondamentale D</u>. Viceversa se p divide D, allora si vede facilmente che D è residuo quadratico di $4p$. Infatti se $p = 2$ siamo certamente nel caso $D = 4d$ ed è $D \equiv 0 \pmod 4$, quindi $D \equiv 0 \pmod 8$ ovvero $D \equiv 4 \pmod 8$, e la congruenza (3) si soddisfa con $r = 0$ ovvero con $r = 2$. Se poi p è dispari, siccome $D \equiv 0 \pmod 4$ ovvero $D \equiv 1 \pmod 4$, si soddisfa la (3) nel primo caso con $r = 0$, nel secondo con $r = p$ (perchè $p^2 \equiv 1 \pmod 4$). Così quando p divide D, siamo nel caso (4), cioè (p) è decomponibile. Ma ora vogliamo far vedere che i due ideali P, P' sono, in questo caso, necessariamente eguali. Poichè infatti π è divisibile per P, e π' per P', mentre r è divisibile per p, il numero

$$\pi = r - \pi'$$

è anche certamente divisibile per P'. Se dunque fosse $P' \neq P$, sarebbe π divisibile per $PP' = (p)$, il che non è.

Per riassumere questi risultati relativi alla decom

posizione dei numeri primi ordinari p in fattori ideali, nel corpo quadratico $K(\theta)$, distinguiamo secondo che $p=2$ ovvero p è dispari.

1°. Se $p=2$ ed è $d \equiv 2,3 \pmod 4$ allora p entra in $D \equiv 4d \equiv 0 \pmod 4$ e per conseguenza l'ideale (2) è il quadrato P^2 di un ideale primo. Se invece $d \equiv 1 \pmod 4$, allora $D = d$ può essere $\equiv 1 \pmod 8$, ovvero $\equiv 5 \pmod 8$; nel primo caso D è residuo di $4p=8$, nel secondo non residuo. E quindi nel primo caso (2) si scinde nel prodotto di due ideali primi diversi P, P' di 1° grado, nel secondo (2) è un ideale primo di secondo grado. Riassumendo abbiamo dunque:

se $d \equiv 2,3 \pmod 4$ l'ideale principale (2) è un quadrato P^2
se $d \equiv 1 \pmod 8$ " $(2) = PP'$
se $d \equiv 5 \pmod 8$ " (2) ideale primo di 2° grado

2°. Sia ora p dispari. Siccome in ogni caso $D^2 \equiv D \pmod 4$, la congruenza $r^2 \equiv D \pmod 4$ è sempre solubile, e la risolubilità della (3) dipende dalla risolubilità dell'altra

$$r^2 \equiv D \pmod p,$$

cioè dall'essere D (ovvero d) residuo o non residuo di p. In questo caso dunque i risultati sono i seguenti

se p divide d l'ideale principale (p) è un quadrato P^2

se $\left(\frac{d}{p}\right) = +1$ " $(p) = PP'$ (P, P' distinti)

se $\left(\frac{d}{p}\right) = -1$ " (p) ideale primo di 2° grado.

In particolare si osservi: conservano le qualità di numeri primi, anche nel corpo $K(\theta)$, tutti e soli quei numeri primi ordinarii dispari che non dividono il numero fondamentale D e dei quali D è non residuo quadratico. Un contegno affatto speciale hanno invece, come si vede, i numeri primi che entrano in D, come quadrati di ideali primi.

Essi sono qui per $n = 2$ i numeri primi critici.

È facile spingere più oltre la ricerca e procurarsi tutti gli ideali primi del corpo quadratico mediante la costruzione effettiva delle loro basi. Basterà considerare uno dei casi, per es. quello in cui $d \equiv 3 \pmod 4$, indi $D = 4d$, nel quale tutti gli interi del corpo $K(\sqrt{d})$ hanno la forma

$$\alpha = x + y\sqrt{d} \qquad (x, y \text{ razionali interi}),$$

e si ha $N(\alpha) = x^2 - dy^2$. Ogni numero primo razionale p o dà luogo già all'ideale principale primo $(p) = P$, o è il quadrato di un ideale primo

$$(p) = P^2,$$

ovvero è il prodotto di due ideali primi diversi coniugati

$$(p) = PP'.$$

In ogni caso appartiene all'ideale P (ovvero P') il numero primo p, ed ogni altro numero α di P, ha $N(\alpha)$ divisibile per p. Viceversa se $N(\alpha) = x^2 - dy^2$ è divisibile per p, allora nei primi due casi α è certamente in P, nel terzo se non appartiene a P appartiene a P'.

Nel primo caso si ha già una base dell'ideale $P = (p)$ nei due numeri

$$\alpha_1 = p, \quad \alpha_2 = p\sqrt{d}.$$

Nel secondo, essendo p divisore di $D = 4d$, la condizione $N\alpha = x^2 - dy^2 \equiv 0 \pmod{p}$ dà semplicemente $x \equiv 0 \pmod{p}$ se p è dispari, e invece $x \equiv y \pmod{2}$ se $p = 2$; perciò abbiamo

$$(2) = P^2 \quad \text{con} \quad P = [2, 1+\sqrt{d}]$$

$$(p) = P^2 \quad \text{con} \quad P = [p, \sqrt{d}] \quad \text{per } p \text{ dispari divisore di } d.$$

Nel terzo caso infine, che ha luogo soltanto per $\left(\frac{d}{p}\right) = +1$ (p dispari), se si indica con a una radice della congruenza

$$a^2 \equiv d \pmod{p},$$

il prodotto

$$(a+\sqrt{d})(a-\sqrt{d})$$

è divisibile per P (e per P'), quindi uno dei fattori è certamente in P, ma non l'altro, perchè la loro somma $2a$ non è divisibile per P (per p). Se chiamiamo P quello dei due fattori primi ideali in cui entra $a+\sqrt{d}$, abbiamo in questo caso

$$(p) = PP' \quad \text{con} \begin{cases} P = [p,\ a+\sqrt{d}] \\ P' = [p,\ a-\sqrt{d}] \end{cases} \quad a^2 \equiv d \pmod{p}$$

Se come esempio numerico riprendiamo il caso $d=-5 \equiv 3 \pmod 4$, $D=-20$ che è quello da cui siamo partiti al § 7, qui abbiamo i due numeri primi critici 2 e 5 fattori di D che sono quadrati di ideali primi

$$(2) = P^2 \qquad \text{con} \quad P = [2,\ 1+i\sqrt{5}]$$

$$(5) = Q^2 \qquad \text{con} \quad Q = [5,\ i\sqrt{5}]$$

Sono decomponibili in due ideali primi coniugati nel corpo $K(i\sqrt{5})$ quei numeri primi p di cui -5 è residuo $\left(\frac{-5}{p}\right)=+1$, cioè i numeri p contenuti nelle progressioni aritmetiche

$$p = 20h+1,\ 20h+3,\ 20h+7,\ 20h+9,$$

così per es.

$$(3) = RR' \qquad R = [3,\ 1+i\sqrt{5}] \qquad R' = [3,\ 1-i\sqrt{5}]$$

$$(7) = SS' \qquad S = [7,\ 3+i\sqrt{5}] \qquad S' = [7,\ 3-i\sqrt{5}]$$

$$(23) = TT' \qquad T = [23,\ 8+i\sqrt{5}] \qquad T' = [23,\ 8-i\sqrt{5}]$$

$$(41) = UU' \qquad U = [41,\ 6+i\sqrt{5}] \qquad U' = [41,\ 6-i\sqrt{5}]$$

ecc. ecc.

Effettuata la decomposizione dei numeri primi razionali nel corpo nei loro ideali primi, la risoluzione di ogni altro intero α del corpo si eseguisce risolvendo la norma $N(\alpha)$ nei suoi fattori primi p e gli ideali primi in cui α si risolve saranno esclusivamente quelli dei numeri p, dove ogni volta, se $(p) = PP'$, sarà facile decidere se in α entri P o P' o in tutti due. Così per es.

$$N(2+i\sqrt{5}) = 9$$

e per ciò il numero $2+i\sqrt{5}$ non può avere altri ideali primi che R o R', non tutti due perchè non è divisibile per 3. Effettivamente esso è contenuto in R' essendo $= 3-(1-i\sqrt{5})$, dunque

$$(2+i\sqrt{5}) = R'^2, \qquad (2-i\sqrt{5}) = R^2.$$

Invece $N(1+i\sqrt{5}) = 6$; quindi $1+i\sqrt{5}$ come contenuto insieme in P e R è divisibile per tutti due ed eguale

al loro prodotto

$$(1+i\sqrt{5}) = PR\ ,\quad (1-i\sqrt{5}) = PR'.$$

Ancora $N(4+i\sqrt{5}) = 21$, indi $4+i\sqrt{5}$ prende un fattore da 3 e uno da 7, e si vede subito che esso appartiene ad R perchè è $= 3+(1+i\sqrt{5})$ e a S' come $= 7-(3-i\sqrt{5})$, indi

$$(4+i\sqrt{5}) = RS'\ ,\quad (4-i\sqrt{5}) = R'S,\ \text{ecc.}$$

§ 33

Equivalenza di ideali - Classi di ideali.

Riprendendo la teoria generale degli ideali, ci volgiamo ora a stabilire una nozione di fondamentale importanza, quella della loro equivalenza.

Premettiamo un lemma che fa conoscere un minimo per le norme dei numeri α contenuti in un ideale qualunque A. In ogni caso, essendo α divisibile per A, è $|N\alpha|$ divisibile per NA, indi $|N\alpha| \geq NA$; anzi il segno d'eguaglianza vale soltanto quando A coincide coll'ideale principale (α) [perchè se $(\alpha) = AB$ in tal caso $NB = 1$ e B coincide coll'ideale unità O]. Ora stabiliamo il teorema:

a) In ogni ideale A sono contenuti dei numeri α

<u>la cui norma non supera $NA\sqrt{(D)}$, dove D è il numero fondamentale del corpo.</u>

Questa è una facile conseguenza del teorema (III) § 16 di Minkowski sulle forme lineari. Prendiamo infatti una base $[\alpha_1^{(1)}, \alpha_2^{(1)} \dots \alpha_n^{(1)}]$ dell'ideale A, alla quale facciamo corrispondere la forma lineare

$$f_1 = \alpha_1^{(1)} x_1 + \alpha_2^{(1)} x_2 + \dots + \alpha_n^{(1)} x_n \ ;$$

questa f_1, quando alle x_i si attribuiscano valori razionali interi, dà i numeri α dell'ideale A. Consideriamo allora le n forme lineari

$$f_i = \alpha_1^{(i)} x_1 + \alpha_2^{(i)} x_2 + \dots + \alpha_n^{(i)} x_n \qquad (i = 1, 2, \dots n)$$

formate coi numeri coniugati $\alpha^{(i)}$ di $\alpha^{(1)}$, divise al solito, come al § 17, in r forme reali ed s coppie di complesse coniugate. Indicando con Ω il modulo del determinante $|\alpha_k^{(i)}|$ di queste forme, si può dare alle x_i, pel citato teorema di Minkowski, tali valori interi non tutti nulli che risulti

$$(1) \qquad |f_1|\,|f_2| \cdots |f_n| \leq \Omega .$$

Ma allora f_1 diventa un numero intero α, non nullo, di A e a sinistra in (1) abbiamo il valore assoluto (modulo) di $N\alpha$; d'altra parte il quadrato del

detto determinante $|\alpha_k^{(i)}|$ non è che il discriminante $\Delta(\alpha_1, \alpha_2, \cdots \alpha_n)$ della base di A e siccome (§ 24 formola (I))

$$\Delta(\alpha_1, \alpha_2 \cdots \alpha_n) = \mathfrak{D}(N(A))^2,$$

risulta

$$\Omega = \sqrt{|\Delta|} = NA.\sqrt{|\mathfrak{D}|},$$

indi il numero α trovato in A soddisfa alla condizione $|N\alpha| \leq NA\sqrt{|\mathfrak{D}|}$, come si voleva.

Per venire alla nozione di equivalenza di ideali, ricordiamo il teorema fondamentale A) del § 25, secondo il quale ogni ideale A può convertirsi in un ideale principale solo che si moltiplichi A per un conveniente ideale; anzi, se si tiene presente l'ulteriore teorema C) del § 28, vediamo che di tali ideali, che convertono A in ideale principale, ne esistono infiniti. Per abbreviare li chiameremo tutti <u>ideali moltiplicatori</u>, o semplicemente moltiplicatori di A, e li indicheremo con $\mathcal{M}$.

Supponiamo che i due ideali A, B abbiano un moltiplicatore comune $\mathcal{M}$, talchè $A\mathcal{M}$, $B\mathcal{M}$ siano due ideali principali, diciamo

$$(1) \qquad A\mathcal{M} = (\alpha) \quad , \quad B\mathcal{M} = (\beta).$$

Se segue

$$(\beta) A \mathcal{M} = (\alpha) B \mathcal{M}$$

e per ciò (a) § 25)

$$(2) \qquad (\beta) A = (\alpha) B \, .$$

Dalla (1) segue dunque la (2). Ma viceversa, se sussiste la (2), un qualunque moltiplicatore $\mathcal{M}'$ di A è anche un moltiplicatore per B. E infatti se $A\mathcal{M}'$ è un ideale principale, diciamo

$$A \mathcal{M}' = (\alpha') \, ,$$

allora moltiplicando la (2) per $\mathcal{M}'$, viene

$$(\beta)(\alpha') = (\alpha) . B \mathcal{M}' .$$

Dunque $(\beta)(\alpha')$ è divisibile per (α), cioè il numero $\beta\alpha'$ per α e se poniamo

$$\beta\alpha' = \rho\alpha \qquad (\rho \text{ intero}) \, ,$$

ne risulta $(\beta)(\alpha') = (\alpha)(\rho)$, indi

$$(\alpha)(\rho) = (\alpha) B \mathcal{M}' \, , \quad B \mathcal{M}' = (\rho) \, ,$$

cioè $\mathcal{M}'$ converte anche B in un ideale principale. Segue di qui che se due ideali hanno un moltiplicatore comune, tutti i moltiplicatori dell'uno sono anche moltiplicatori dell'altro. Ed allora poniamo la seguente definizione:

1) Due ideali A, B si dicono equivalenti quando hanno uno, e quindi tutti i moltiplicatori comuni (Dedekind).

Come abbiamo visto, l'equivalenza così definita di due ideali equivale perfettamente alla relazione (2), la quale può quindi assumersi come seconda definizione per l'equivalenza:

2) Due ideali A, B sono equivalenti se esistono due ideali principali (α), (β) tali che si abbia la (2)

$$(\beta) A = (\alpha) B .$$

Anche si può dire che se due ideali sono equivalenti, vi ha una corrispondenza biunivoca fra i loro numeri tale che i numeri corrispondenti sono in rapporto costante. Riferendosi alle basi dei due ideali, è chiaro che da una base dell'uno $[\alpha_1, \alpha_2 \cdots \alpha_n]$ si ottiene una base dell'altro moltiplicando i numeri della base per un numero frazionario $\frac{\beta}{\alpha}$ che li converta in numeri interi $[\beta_1, \beta_2 \cdots \beta_n]$, e adottare quest'altra definizione (Minkowski):

3) Due ideali A, B sono equivalenti se hanno basi proporzionali.

Per significare l'equivalenza di due ideali adotteremo la scrittura

$$A \sim B,$$

e dall'una o dall'altra delle definizioni dedurremo subito che valgono le proprietà elementari seguenti:

α) (proprietà di transitività) Se due ideali sono equivalenti ad un terzo sono equivalenti fra loro, ossia da

$$A \sim B\,, \quad A \sim C\,, \quad \text{segue} \quad B \sim C.$$

Difatti, avendo B, C a comune i moltiplicatori con A, hanno anche gli stessi moltiplicatori fra loro.

β) Tutti gli ideali principali e soltanto questi sono equivalenti all'ideale unità.

Difatti ogni ideale principale ha evidentemente tutti gli altri ideali principali come moltiplicatori; e viceversa se un ideale A ha un moltiplicatore principale è esso stesso principale, perchè da

$$A(\beta) = (\alpha)$$

segue (α) divisibile per (β), cioè $(\alpha) = (\beta)(\rho)$, $A(\beta) = (\beta)(\rho)$, indi $A = (\rho)$.

γ) Se $A \sim B$, $C \sim D$, si ha anche $AC \sim BD$.

Difatti se M è un moltiplicatore comune ad A, B,

ed M' un moltiplicatore di C, D, è MM' moltiplicatore comune di AC, BD, che sono quindi equivalenti.

δ) <u>Da $AC \sim BC$ segue $A \sim B$</u>. E infatti, ricorrendo qui alla (2), avremo

$$(\beta).AC = (\alpha).BC$$

$$(\beta)A = (\alpha)B \quad , \quad \text{cioè} \quad A \sim B.$$

In base alla proprietà transitiva a), tutti gli ideali possono ripartirsi in <u>classi</u>, collocando in una medesima classe tutti gli ideali equivalenti ad uno stesso, e per ciò fra loro. Qualsiasi ideale, estratto da una classe, la determina completamente e si dirà un rappresentante della medesima, così per es. l'ideale unità è un rappresentante di tutta la classe degli ideali principali, che si dirà la classe principale e si indicherà con <u>1</u>. In generale col simbolo K indicheremo una classe di ideali. Ora dimostriamo:

<u>In qualunque classe K esiste almeno un ideale A la cui norma non supera $\sqrt{(D)}$.</u>

Prendasi un ideale qualunque di K ed un suo moltiplicatore M che sarà anche moltiplicatore di

di tutti e soli gli ideali in K. In questo ideale M esiste, pel teorema a) al principio del §, un numero μ tale che

$$(3) \qquad |N\mu| \leq N(M).\sqrt{(D)}.$$

Ma μ è divisibile per M, poniamo

$$(\mu) = AM$$

ed allora A, avendo il moltiplicatore M, appartiene a K. D'altronde dalla precedente si ha

$$|N\mu| = N(A).N(M),$$

indi sostituendo in (3)

$$NA \leq \sqrt{(D)},$$

come si voleva.

Se questo risultato si confronta coll'altro stabilito al § 29 teorema c), che è finito il numero degli ideali colla stessa norma, si arriva a quest'altro capitale risultato:

A) Il numero delle classi d'ideali è finito. In altre parole in qualunque corpo algebrico esiste un numero finito d'ideali fra loro non equivalenti.

Indichiamo con h questo numero finito delle classi, e le classi stesse con

$$(4) \qquad K_1, K_2, \cdots K_h ;$$

la determinazione di questo numero h, inerente al corpo $K(\theta)$, costituisce un problema di rilevante importanza per la teoria, ma lo potremo affrontare soltanto più tardi, coi metodi dell'aritmetica analitica. [Capitolo seguente].

Intanto le proprietà γ) e δ), relative alla equivalenza di ideali, si possono subito trasportare in una altra nozione: quella di composizione delle classi. Se K, K' sono due qualunque delle classi e da K si estraggono due ideali qualunque A, B, da K' altri due ideali $A'B'$, siccome

$$A \sim B, \quad A' \sim B'$$

ne segue

$$AA' \sim BB',$$

e per ciò, variando comunque A in K e A' in K', tutti gli ideali prodotti AA' appartengono ad una sola e medesima classe $\bar{K}$, che si dice il prodotto delle due K, K' e si scrive

$$\bar{K} = KK'$$

Il prodotto così definito per due classi di ideali è

manifestamente indipendente dall'ordine dei fattori:

$$KK' = K'K.$$

Così si definiscono anche i prodotti di quante si vogliano (fra le h classi), ciascuna ripetuta quante volte si voglia, e per questi prodotti valgono manifestamente le leggi commutativa, associativa, la legge di sommazione degli esponenti ecc. Anche è da osservarsi che fra le h classi (4) vi è la principale, che si potrà supporre la prima $K_1 \doteq 1$; inoltre ogni classe K individua la sua classe inversa (o dei moltiplicatori) che composta colla prima dà la classe principale 1. Questa inversa si indicherà con K^{-1} e si riguarderà come la potenza con esponente -1 di K. Indicando le classi con lettere $H, K, L \ldots$ è chiaro che da

$$(5) \qquad H = H'$$

segue, qualunque sia K

$$(6) \qquad HK = H'K$$

ma anche inversamente dalla (6) segue la (5), come si vede moltiplicando questa per K^{-1}. Queste semplici osservazioni dimostrano che alla composizione

delle classi si possono applicare i concetti generali dei gruppi (finiti) di operazioni, ciò che andiamo ora a considerare più da vicino.

§ 34

Il gruppo di composizione e i caratteri delle classi.

Se si moltiplicano tutte le h classi

a) $K_1, K_2, \dots K_h$

per una di esse K_i, le classi

1) $K_1 K_i, K_2 K_i, \dots K_h K_i$,

a causa delle proprietà elementari osservate, coincidono in altro ordine colle a). L'effetto della moltiplicazione di tutte le h classi per una di esse K_i è dunque di indurre sulle classi una sostituzione S_i.

$$S_i = \begin{pmatrix} K_1 K_i, K_2 K_i \dots K_h K_i \\ K_1, K_2 \dots K_h \end{pmatrix}$$

sulle h lettere o simboli $K_1, K_2 \dots K_h$. Classi diverse K_i, K_j come moltiplicatrici producono manifestamente sostituzioni diverse S_i, S_j, e la moltiplicatrice prodotto $K_i K_j = K_\ell$ delle due produce la sostituzione composta o prodotto $S_i S_j = S_\ell$.

Per ciò alle h classi $K_1, K_2, \ldots K_h$ corrispondono (biunivocamente) le h sostituzioni

$$c) \qquad S_1, \; S_2, \ldots S_h \, ,$$

fra le quali vi è l'identità $S_1 = 1$ corrispondente alla classe principale K_1. Le h sostituzioni c) formano quindi un gruppo di h sostituzioni due a due permutabili: un gruppo Abeliano di ordine h. Senza ricorrere alla teoria generale dei gruppi Abeliani, stabiliremo direttamente le proprietà di questo gruppo che diciamo il gruppo di composizione delle classi.

In primo luogo osserviamo che una classe qualunque K può comporsi successivamente con sè stessa, e si formano così le successive potenze

$$K, K^2, K^3, \ldots ;$$

ma siccome vi sono solo h classi distinte, da un certo punto in poi queste potenze si ripetono. Ora se supponiamo

$$K^{\alpha+\beta} = K^\alpha,$$

cioè

$$K^\alpha \cdot K^\beta = K^\alpha,$$

ne segue che K^β è la classe principale 1, che indicheremo

no anche con K^0. Se β è il più piccolo esponente intero positivo pel quale $K^\beta = 1$, si dirà che β è il periodo di K. La potenza $K^{\beta-1} = K^{-1}$ è la classe inversa di K, e definiamo le potenze di K con esponente negativo $-n$ colla convenzione,

$$K^{-n} = (K^{-1})^n.$$

Ne risulta subito che due potenze qualunque K^m, $K^{m'}$ sono eguali allora ed allora soltanto che $m \equiv m'$ (mod β). In particolare $K^m = 1$ solo quando m è divisibile pel periodo β.

Le β potenze di K

$$K^0 = 1, K, K^2, \dots K^{\beta-1}$$

sono tutte diverse fra loro, ma componendone due qualunque, distinte od eguali, si ha sempre ancora una di esse. Per ciò si dice che esse formano il gruppo (ciclico) $(1, K, K^2, \dots K^{\beta-1})$. In generale se, estraendo dalle h classi a) un certo numero r di esse

$$d) \qquad H_1, H_2, \dots H_r,$$

queste formano un gruppo fra loro, cioè componendone due qualunque diverse od eguali, si ha sempre una delle d), diremo che le d) costituiscono un sot-

togruppo (H) di ordine r del gruppo totale (K). In *d)* è compresa qualunque potenza di una sua classe H, e per ciò anche la classe principale 1, onde segue che in d), insieme ad una H, figura anche la sua inversa H^{-1}. È facile dimostrare che: *l'ordine r di un sottogruppo (H) divide l'ordine h del gruppo (K)*. Questo è ovvio nel caso che (H) coincide con (K), $h = r$. Se $h > r$ prendasi da (K) una classe K non contenuta in (H), e si formino le r classi

$$d') \qquad H_1K,\ H_2K,\ \dots H_rK,$$

le quali sono tutte diverse, perchè da $H_iK = H_jK$ seguirebbe $H_i = H_j$; ma inoltre distinte dalle d), perchè queste formano gruppo. E infatti da

$$H_iK = H_j$$

segue $K = H_i^{-1}H_j = H_l$, contro l'ipotesi. Le d) d') insieme formano $2r$ classi diverse, per ciò $h \geqq 2r$. Se $h = 2r$ l'osservazione è verificata; se $h > 2r$ prendasi una classe K' fuori delle d), d') e si formino le r nuove classi

$$H_1K',\ H_2K',\ \dots H_rK'$$

che saranno distinte dalle $2r$ precedenti; per ciò $h \geqq 3r$. Così continuando, le h classi vengono distribuite in un

un certo numero q di orizzontali, contenenti ciascu-na r classi, ed è perciò $h = qr$, c.d.d.

Come corollario di questo teorema si ha: Il periodo β di qualunque classe è un divisore del numero h delle classi (perchè β è l'ordine di un sottogruppo ciclico). In altri termini qualunque classe K elevata ad h dà la classe principale

$$K^h = 1.$$

Si osservi che se da K si estrae un qualunque ideale A la potenza A^h (eventualmente una d'esponente minore, divisore di h) è certamente un ideale principale. Ne segue che qualunque ideale A è convertito in un ideale principale da A^{h-1}, che è quindi un moltiplicatore di A.

Rispetto ai periodi delle classi valgono le proprietà seguenti:

α) Se β è il periodo di K, il periodo β' di una sua potenza K^m è dato da $\beta' = \frac{\beta}{\varepsilon}$ dove ε è il massimo comun divisore di (m, β). E infatti da $K^{m\beta'} = 1$ segue $m\beta' \equiv 0 \pmod{\beta}$, $\frac{m}{\varepsilon}\beta' \equiv 0 \pmod{\frac{\beta}{\varepsilon}}$, $\beta' \equiv 0 \pmod{\frac{\beta}{\varepsilon}}$, e d'altra parte si ha effettivamente

$$(K^m)^{\frac{\beta}{\varepsilon}} = K^{\frac{m}{\varepsilon}\cdot\beta} = 1$$

β) Se i periodi β, β' di due classi K, K' sono primi fra loro, il periodo della classe prodotto KK' è il prodotto dei due periodi $\beta\beta'$. È infatti se $(KK')^m = 1$, abbiamo

$$K^m = K'^{-m};$$

la classe a sinistra ha per α) un periodo divisore di β, quella a destra un periodo divisore di β', dunque il periodo di queste due classi eguali è necessariamente $=1$, cioè

$$K^m = K'^m = 1.$$

L'esponente m deve dunque essere divisibile tanto per β che per β', indi pel loro prodotto, e d'altronde si ha già

$$(KK')^{\beta\beta'} = K^{\beta\beta'} . K'^{\beta\beta'} = 1.$$

Questa proprietà β) è immediatamente estendibile a quante si vogliano classi i cui periodi siano primi fra loro due a due.

γ) Tutti i periodi delle varie classi dividono il massimo di essi.

Sia β il massimo di tutti i periodi, e K una classe di questo periodo. Se un'altra classe K' avesse un periodo β' non divisore di β, potremmo formare una classe di periodo $> \beta$. E difatti se β' non divide β vi sa-

rà in β' almeno un fattore primo p che entrerà in β' ad una potenza maggiore che non in β, poniamo alla potenza $r+s$ in β', alla potenza s in β, talchè $r>0$, $s \geq 0$.

Allora se poniamo

$$\beta = p^r \cdot \rho \ , \quad \beta' = p^{r+s} \cdot \rho' ,$$

saranno ρ, ρ' non più divisibili per p. Ora le due classi

$$K^{p^r} \quad , \quad K'^{\rho'}$$

hanno i rispettivi periodi

$$\rho \quad , \quad p^{r+s}$$

primi fra loro. Per ciò la classe prodotto avrebbe il periodo $p^{r+s}\rho > \beta$, contro l'ipotesi.

Le proprietà precedenti si estendono facilmente dai periodi assoluti delle classi ai periodi relativi rispetto ad un qualunque sottogruppo $H)$ di (K) che si definiscono nel modo seguente. Dicesi periodo relativo della classe K rispetto al sottogruppo (H) quel più piccolo esponente β_0 intero positivo pel quale K^{β_0} appartiene al sottogruppo (H). In ogni caso il periodo relativo β_0 è divisore dell'assoluto β.

Fondandosi su queste nozioni, si arriva a stabilire quanto segue:

Fra le classi se ne può scegliere un certo numero r, diciamo

$$H_1, H_2, \dots H_r$$

di rispettivi periodi

$$h_1, h_2, \dots h_r,$$

ciascuno divisore del precedente, e tali che $h = h_1 . h_2 \dots h_r$; ogni classe K è rappresentabile in uno ed in un sol modo sotto la forma

$$K = H_1^{\alpha_1} H_2^{\alpha_2} \dots H_r^{\alpha_r},$$

dove ciascun esponente α_i può avere uno dei valori $0, 1, 2, \dots h_i - 1$.

Un tale sistema $H_1, H_2, \dots H_r$ di classi formano una così detta base del gruppo e i numeri $h_1, h_2, \dots h_r$ sono i relativi invarianti. Per ogni classe K sono perfettamente determinati i relativi esponenti $\alpha_1, \alpha_2, \dots \alpha_r$ e i valori delle seguenti radici h^{me} dell'unità

$$\chi_1(K) = e^{\frac{2\pi i \alpha_1}{h_1}}, \quad \chi_2(K) = e^{\frac{2\pi i \alpha_2}{h_2}}, \quad \chi_r(K) = e^{\frac{2\pi i \alpha_r}{h_r}}$$

dànno i così detti caratteri della classe K, o anche di ogni ideale A contenuto nella classe K. Dalla definizione di questi caratteri risulta subito che se K, K' sono due

classi, ciascuno degli r caratteri soddisfa alla relazione

$$\chi(KK') = \chi(K) \cdot \chi(K')$$

§ 35

Gli ideali come numeri esistenti in corpi ampliati - Massimo comun divisore di due interi algebrici α, β.

Il fatto sopra rilevato, che qualunque ideale A, elevato al numero h delle classi, dà un ideale principale, può mettersi in relazione col concetto primitivo di Kummer dei fattori ideali nel modo seguente (Dedekind).

Essendo

$$A^h = (\rho)$$

se poniamo

$$\rho_0 = \sqrt[h]{\rho},$$

anche ρ_0 è un intero algebrico (§ 10), però generalmente fuori del corpo $K(\theta)$. Se ρ_0 appartiene a $K(\theta)$, si ha

$$A^h = (\rho_0^h) = (\rho_0)^h,$$

quindi $A = (\rho_0)$ cioè A stesso è principale. [In generale, ricorrendo alla decomposizione in ideali primi, è evidente che se due ideali A, B hanno eguale potenza r^{ma} sono eguali]. Ma anche se ρ_0 è fuori di $K(\theta)$, si vede che l'idea-

le A consta di tutti e soli i numeri interi di $K(\theta)$ che sono divisibili per l'intero algebrico μ_0: Difatti se α è un qualunque numero di A, la potenza α^h è in A^h, indi divisibile per $\mu = \mu_0^h$; dunque $\left(\frac{\alpha}{\mu_0}\right)^h$ è un intero algebrico, per ciò anche $\frac{\alpha}{\mu_0}$, cioè qualunque α in A è divisibile per μ_0. Ma anche inversamente, se α è un intero di $K(\theta)$ divisibile per μ_0, sarà α^h divisibile per $\mu_0^h = \mu$, cioè α^h per A^h, indi α per A, e il numero α è in A.

Così adunque, ad ogni ideale A non principale in $K(\theta)$ si può sostituire un intero algebrico perfettamente determinato μ_0, che non esiste in $K(\theta)$, ma fuori di $K(\theta)$, e i suoi multipli in $K(\theta)$ sono precisamente i numeri di A. In particolare, nella decomposizione di un ideale principale (α) nei suoi ideali primi

$$(\mu) = P_1^{n_1} P_2^{n_2} \cdots P_r^{n_r},$$

si può sostituire ciascuno di questi P_i col corrispondente intero algebrico μ_i, generalmente fuori di $K(\theta)$, e la corrispondente decomposizione del numero μ

$$\mu = \mu_1^{n_1} \mu_2^{n_2} \cdots \mu_r^{n_r}.$$

Questi nuovi numeri $\mu_1, \mu_2, \ldots \mu_r$ sono generalmente non esistenti in $K(\theta)$, ma esistono fuori di $K(\theta)$, e fu

appunto nel riconoscere la loro necessaria introduzione come elementi fittizi in $K(\theta)$, per ristabilire le leggi della divisibilità, che si presentarono a Kummer come fattori ideali.

Tutte le volte che si abbia $h=1$, ogni ideale è principale, e valgono le leggi ordinarie di divisibilità senza introduzione di fattori ideali. Per es. nel caso dei corpi quadratici si ha $h=1$ pei valori seguenti di d

corpi immaginarii $d = -1, -2, -3, -7, -11, -19, -43, -67$

corpi reali $d = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 33$ ecc.

Quando $h=2$ il quadrato di qualunque ideale è un ideale principale e i fattori ideali (rispetto a $K(\theta)$) da introdurre sono numeri effettivi esistenti in corpi più ampi biquadratici. Così pei corpi quadratici si ha $h=2$ pei seguenti valori di d

corpi immaginari $d = -5, -6, -10, -13, -15, -22, -35, -37$ ecc.

corpi reali $d = 10, 15, 26, 30, 34$, ecc.

Ancora nei corpi quadratici è $h=3$ nei casi

corpi immaginari $d = -23, -31, -59, -83$ ecc.

corpi reali $d = 31, 79, \ldots\ldots$;

qui i fattori ideali da introdurre sono numeri esistenti

in corpi di 6° grado.

Dalle considerazioni superiori Dedekind ha tratto un'altra importante conseguenza colla quale si viene a stabilire un concetto assoluto di massimo comun divisore di due interi algebrici α, β comunque dati. Dimostriamo:

<u>Per due interi algebrici α, β comunque dati esiste un altro intero algebrico δ, definito a meno di un fattore unità, da riguardarsi come loro massimo comun divisore, caratterizzato dalla proprietà che esistono due altri interi algebrici ξ, η tali che si abbia:</u>

$$(1) \qquad \alpha\xi + \beta\eta = \delta.$$

Per dimostrare questo osserviamo che, qualunque siano α, β, può sempre trovarsi un corpo algebrico finito $K(\theta)$ nel quale siano ambedue contenuti. Questa proprietà, che sarà estesa più oltre (v. § 39) ad un numero qualsiasi di interi algebrici, dipende dalle proprietà fondamentali dei numeri algebrici (§§ 9 e 10) ed è quella appunto che sta alla base della teoria di Galois.

In questo corpo $K(\theta)$, del quale il numero delle classi sia h, consideriamo i due ideali principali $(\alpha), (\beta)$, i quali avranno un ideale massimo comun divisore,

che indichiamo con D, e poniamo

$$(\alpha) = AD \quad , \quad (\beta) = BD,$$

dove i due ideali A, B sono primi fra loro. I tre ideali A^h, B^h, D^h sono principali, scriviamo

$$A^h = (\lambda) \quad , \quad B^h = (\mu) \quad , \quad D^h = (\rho),$$

dove gli interi λ, μ, ρ sono in $K(\theta)$, e i primi due sono primi fra loro, tali essendo A^h, B^h. Ne consegue

$$(\alpha)^h = (\lambda)(\rho) \quad , \quad (\beta)^h = (\mu)(\rho),$$

cioè

$$\alpha^h = \lambda\rho \quad , \quad \beta^h = \mu\rho$$

Siccome λ, μ sono primi fra loro (cioè l'ideale (λ, μ) coincide coll'ideale unità), esistono in $K(\theta)$ due numeri interi λ', μ' tali che si abbia

$$\lambda\lambda' + \mu\mu' = 1$$

indi moltiplicando per ρ

$$(2) \qquad \alpha^h\lambda' + \beta^h\mu' = \rho.$$

Introduciamo ora l'intero algebrico

$$\delta = \sqrt[h]{\rho} \quad , \quad \rho = \delta^h$$

[il quale è generalmente fuori di $K(\theta)$], e sarà δ un divisore comune di α, β, poichè divide D. Sarà dunque δ^{h-1} divisore comune di $\alpha^{h-1}, \beta^{h-1}$ e potremo porre

$$\alpha^{k-1}\lambda' = \delta^{k-1}\xi \,, \quad \beta^{k-1}\mu' = \delta^{k-1}\eta \,,$$

con ξ, η interi algebrici. Sostituendo nella (2), questa diventa

$$\alpha\delta^{k-1}\xi + \beta\delta^{k-1}\eta = \delta^{k} \,,$$

e divisa per δ^{k-1} dà la relazione annunciata (1).

Ora risulta da questa (1) che δ è un divisore comune di α, β (perchè nel corpo a cui appartengono α, β, ξ, η, il numero δ si compone linearmente con α, β) e d'altronde, per la (1), stessa, ogni intero algebrico che divide simultaneamente α, β divide anche δ; questo numero δ è dunque da dirsi appunto il <u>massimo comun divisore</u> di α, β. E si osservi che se per altri due interi algebrici ξ_1, η_1 si ha

$$\alpha\xi_1 + \beta\eta_1 = \delta_1 \,,$$

allora δ divide δ_1 e δ_1 divide δ, e per ciò differiscono solo di un fattore unità (sono associati).

In particolare la nozione di numeri interi algebrici primi fra loro acquista così un significato <u>assoluto</u>. I due interi algebrici α, β saranno primi fra loro quando esista una coppia ξ, η di altri interi

algebrici tali che si abbia

$$\alpha\xi + \beta\eta = 1.$$

§ 36.

I numeri frazionari σ in $K(\theta)$ come coordinati alle classi di ideali. – Teorema di Hurwitz.

Le considerazioni svolte nel § precedente stanno in intima relazione colla proprietà già dimostrata al § 28, col teorema D), potersi considerare ogni ideale in $K(\theta)$ quale massimo comun divisore di due numeri α, β, in $K(\theta)$, dei quali anzi uno può esser preso ad arbitrio.

Ora domandiamoci: quando è che due coppie di numeri (α, β), (α', β') in $K(\theta)$ individuano il medesimo ideale

$$A = (\alpha, \beta) = (\alpha', \beta') \, ?$$

A questo risponde il teorema di Hurwitz:

Per l'eguaglianza di due ideali (α, β), (α', β') è necessario e sufficiente che α', β' siano legati ad α, β da una sostituzione lineare

$$(3) \qquad \begin{cases} \alpha' = \lambda\alpha + \mu\beta \\ \beta' = \nu\alpha + \rho\beta \end{cases}$$

<u>con coefficienti λ, μ, ν, ρ interi in $K(\theta)$ e di determinante $\lambda\rho - \mu\nu = 1$</u> (<u>sostituzione unimodulare</u>).

Che la condizione sia sufficiente è immediato, perchè se $\lambda\rho - \mu\nu = 1$, risolvendo le (3) si ha inversamente

$$(3^*) \qquad \begin{cases} \alpha = \rho\alpha' - \mu\beta' \\ \beta = -\nu\alpha' + \lambda\beta' \end{cases}$$

e quindi ogni divisor comune di α', β' è anche divisor comune di α, β e inversamente, onde le due coppie hanno lo stesso massimo comun divisore, ed è per ciò $(\alpha, \beta) = (\alpha', \beta')$.

Per dimostrare la necessità della condizione, si indichi come sopra con h il numero delle classi in $K(\theta)$; allora, posto $D = (\alpha, \beta) = (\alpha', \beta')$, è D^h un ideale principale, diciamo come al § precedente

$$D^h = (\gamma)$$

sicchè posto $\delta = \sqrt[h]{\gamma}$, siccome D è il massimo comun divisore di $A = (\alpha)$, $B = (\beta)$, sarà δ massimo comun divisore di α, β, e si avrà secondo la (2) § 35

$$\delta^h = \alpha^h \lambda' + \beta^h \mu'$$

con λ', μ' interi in $K(\theta)$, ovvero ponendo $\alpha^{h-1}\lambda' = \xi$, $\beta^{h-1}\mu' = \eta$:

$$(4) \qquad \delta^h = \alpha\xi + \beta\eta$$

con ξ, η interi in $K(\theta)$ e divisibili per l'intero algebrico δ^{h-1}; similmente

$$(4^*) \qquad \delta^h = \alpha'\xi' + \beta'\eta'$$

con ξ', η' interi in $K(\theta)$ divisibili per δ^{h-1}. Ora pongasi

$$(5) \qquad \begin{cases} \lambda = \dfrac{\alpha'\xi + \beta\eta'}{\delta^h}, & \mu = \dfrac{\alpha'\eta - \alpha\eta'}{\delta^h} \\ \nu = \dfrac{\beta'\xi - \beta\xi'}{\delta^h}, & \rho = \dfrac{\beta'\eta + \alpha\xi'}{\delta^h} \end{cases}$$

e si avrà

$$\begin{cases} \lambda\alpha + \mu\beta = \dfrac{\alpha'(\alpha\xi + \beta\eta)}{\delta^h} = \alpha' \\ \nu\alpha + \rho\beta = \dfrac{\beta'(\alpha\xi + \beta\eta)}{\delta^h} = \beta' \end{cases}$$

che sono le (3). Inoltre

$$\lambda\rho - \mu\nu = \frac{(\alpha\xi + \beta\eta)(\alpha'\xi + \beta\eta')}{\delta^{2h}},$$

cioè per le (4), (4*): $\lambda\rho - \mu\nu = 1$, sicchè altro non resta a provare che λ, μ, ν, ρ sono interi algebrici in $K(\theta)$. Questi numeri sono infatti in $K(\theta)$ perchè a questo corpo appartengono α, β; α', β'; ξ, η; $\xi' \eta'$ e inoltre δ^h; ma di più sono interi perchè α, β; α', β' sono divisibili per δ, mentre ξ, η; ξ', η' sono divisibili per δ^{h-1}. Così il teorema di Hurwitz è dimostrato.

Da questo teorema che dà la condizione necessaria e sufficiente per l'eguaglianza di due ideali (α, β),

(α', β'), è facile ora trarre la condizione perchè due ideali (α, β), (α', β') siano equivalenti. In questo caso infatti esisteranno, pel § 33, due numeri interi ρ, ρ' in $K(\theta)$ tali che si abbia:

$$(\rho)\cdot(\alpha, \beta) = (\rho')\cdot(\alpha', \beta'),$$

cioè

$$(\rho\alpha, \rho\beta) = (\rho'\alpha', \rho'\beta').$$

Pel teorema di Hurwitz è adunque necessario che si abbia

$$(6) \qquad \begin{cases} \rho'\alpha' = \lambda.\rho\alpha + \mu.\rho\beta \\ \rho'\beta' = \nu.\rho\alpha + \rho.\rho\beta \end{cases}$$

dove $\begin{pmatrix} \lambda, \mu \\ \nu, \rho \end{pmatrix}$ è una sostituzione unimodulare con coefficienti λ, μ, ν, ρ interi in $K(\theta)$. Dividendo le (6) e ponendo $\sigma = \frac{\alpha}{\beta}$, $\sigma' = \frac{\alpha'}{\beta'}$, ne deduciamo

$$(I) \qquad \sigma' = \frac{\lambda\sigma + \mu}{\nu\sigma + \rho} \qquad (\lambda\rho - \mu\nu = 1).$$

Viceversa se supponiamo che i due numeri frazionari $\sigma = \frac{\alpha}{\beta}$, $\sigma' = \frac{\alpha'}{\beta'}$ siano legati fra loro da una relazione della forma (I), ponendo il numero frazionario

$$\frac{\lambda\alpha + \mu\beta}{\alpha'} = \frac{\nu\alpha + \rho\beta}{\beta'}$$

sotto una forma comune qualunque $\frac{\rho'}{\rho}$, ne risultano le (6) e, pel teorema di Hurwitz i due ideali (α, β),

(α', β') sono equivalenti. Se adunque ad ogni ideale scritto sotto la forma binaria (α, β), coordiniamo il numero frazionario

$$\sigma = \frac{\alpha}{\beta},$$

e viceversa ad ogni numero frazionario σ, scritto sotto una qualunque delle sue forme $\frac{\alpha}{\beta}$, coordiniamo l'ideale (α, β), e chiamiamo equivalenti due numeri frazionari σ, σ' in $K(\theta)$ quando siano legati da una sostituzione lineare unimodulare (I) con coefficienti interi nel corpo, possiamo concludere:

<u>Condizione necessaria e sufficiente perchè due ideali siano equivalenti è che i rispettivi numeri frazionari coordinati siano equivalenti</u>. E si osservi che, se questa condizione è soddisfatta per due particolari numeri σ, σ' coordinati è soddisfatta per tutte le altre coppie.

Ripartendo adunque i numeri frazionari (e interi) di $K(\theta)$ in <u>classi</u>, col porre nella stessa classe quelli equivalenti ad un medesimo, indi fra loro, questa ripartizione corrisponde perfettamente alla ripartizione degli ideali in classi, cioè a due ideali della

stessa classe corrispondono numeri frazionari equivalenti e viceversa. In particolare tutti gli interi σ, σ' sono equivalenti, avendosi

$$\sigma' = \sigma + (\sigma' - \sigma)$$

ciò che corrisponde alla sostituzione unimodulare $\begin{pmatrix} 1, & \sigma'-\sigma \\ 0 & 1 \end{pmatrix}$, e la classe corrispondente è la classe principale. Si osservi che le sostituzioni unimodulari (I) formano manifestamente un <u>gruppo</u> infinito, e di numeri frazionarii in $K(\theta)$ <u>non equivalenti</u> rispetto a questo gruppo ne esiste un numero finito <u>h</u> dato dal numero delle classi di ideali.

§ 37

Forme decomponibili coordinate agli ideali.

La teoria degli ideali nei corpi algebrici si può anche riguardare come una teoria d'<u>aritmetica razionale</u> introducendo, per un corpo di grado <u>n</u>, certe forme di grado <u>n</u> in <u>n</u> variabili $x_1, x_2 \ldots x_n$ con coefficienti <u>interi ordinarii</u> e che godono della proprietà fondamentale di essere decomponibili nel prodotto di <u>n</u> forme lineari, con coefficienti interi algebrici

appartenenti rispettivamente al corpo $K(\theta)$ ed ai suoi coniugati.

Prendasi un qualunque ideale A e sia

$$[\alpha_1, \alpha_2, \dots \alpha_n]$$

una sua base, che si esprima per la base $[\omega_1, \omega_2, \dots \omega_n]$ del corpo $K(\theta)$ colle formule

$$(1) \qquad \alpha_i = \sum_{k=1}^{k=n} a_{ik}\,\omega_k \qquad (i = 1, 2, \dots n),$$

dove i coefficienti a_{ik} sono <u>interi razionali</u>. Supporremo senz'altro il determinante $|a_{ik}|$ positivo (bastando nel caso contrario cangiare di segno uno dei numeri α_i della base) ed allora avremo (§ 24)

$$\mathcal{N}A = |a_{ik}|.$$

Siccome A è un ideale, qualunque prodotto $\alpha_i\omega_r$ è un numero di A, cioè della forma $h_1\alpha_1 + h_2\alpha_2 + \dots + h_r\alpha_r$ colle $\underline{h}$ interi ordinarii; avremo quindi

$$(2) \qquad \alpha_i\,\omega_r = \sum_{l=1}^{l=n} c_{ir}^{(l)}\,\alpha_l \qquad (i, r = 1, 2, \dots n),$$

dove $c_{ir}^{(l)}$ sono numeri interi razionali, e per la (1) possiamo anche scrivere

$$(3) \qquad \alpha_i\,\omega_r = \sum_{l,k} c_{ir}^{(l)}\,a_{lk}\,\omega_k\,,$$

e più in generale, passando ai numeri coniugati di quelli del corpo

$$(3^*) \qquad \alpha_i^{(s)}\omega_r^{(s)} = \sum_{l,k} c_{ir}^{(l)} a_{lk}\,\omega_k^{(s)} \qquad (s=1,2,\dots n).$$

Indicando ora con $x_1, x_2, \dots x_n$ n variabili, coordiniamo all'ideale A la forma lineare

$$(4) \qquad \varphi = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n ,$$

che per valori interi k_i delle variabili x_i ci darà gli interi $\underline{\alpha}$ dell'ideale A. Dall'essere $\varphi\,\omega_r = \sum_i \alpha_i\,\omega_r\,x_i$ deriva per la (2)

$$\varphi\,\omega_r = \sum_{ilk} c_{ir}^{(l)} a_{lk}\,\omega_k\,x_i .$$

Se introduciamo dunque le n^2 forme lineari a coefficienti interi ordinarii

$$(5) \qquad u_{rl} = \sum_i c_{il}^{(r)} x_i ,$$

possiamo anche scrivere

$$(6) \qquad \varphi\,\omega_r = \sum_{lk} u_{rl}\,a_{lk}\,\omega_k .$$

Il determinante

$$f_r = \begin{vmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ u_{21} & u_{22} & \dots & u_{2n} \\ \dots & \dots & \dots & \dots \\ u_{n1} & u_{n2} & \dots & u_{nn} \end{vmatrix}$$

è una forma di grado $\underline{n}$ nelle variabili $x_1, x_2 \dots x_n$ con <u>coefficienti interi ordinarii</u>, e questa diremo la forma X coordinata all'ideale A (mediante le basi $[\alpha_1\,\alpha_2 \dots \alpha_n]$ di A

e $[\omega_1, \omega_2 \dots \omega_n]$ di O). Dimostriamo che: questa forma X è decomponibile nel prodotto di n forme lineari e precisamente si ha

$$(I) \qquad X = \frac{1}{N(A)} \prod_{s=1}^{s=n} (\alpha_1^{(s)} x_1 + \alpha_2^{(s)} x_2 + \dots + \alpha_n^{(s)} x_n).$$

Per questo osserviamo che, se alle x_i attribuiamo valori interi ordinari k_i, la forma φ diventa un numero intero di A

$$\alpha^{(1)} = \alpha_1^{(1)} h_1 + \alpha_2^{(1)} h_2 + \dots + \alpha_n^{(1)} h_n,$$

e passando ai coniugati si ha in generale

$$\alpha^{(s)} = \alpha_1^{(s)} h_1 + \alpha_2^{(s)} h_2 + \dots + \alpha_n^{(s)} h_n.$$

Ora risulta dalla (6)

$$\alpha^{(s)} \omega_i^{(s)} = \sum_{lk} \bar{u}_{il} a_{lk} \omega_k^{(s)},$$

dove il soprassegno indica che alle x_i si sono sostituiti i numeri interi k_i. Il determinante degli n^2 numeri a sinistra è manifestamente

$$\alpha^{(1)} \alpha^{(2)} \dots \alpha^{(n)} \begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \dots & \omega_n^{(1)} \\ \dots & \dots & \dots & \dots \\ \omega_1^{(n)} & \omega_2^{(n)} & \dots & \omega_n^{(n)} \end{vmatrix} = N(\alpha) \begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \dots & \omega_n^{(1)} \\ \dots & \dots & \dots & \dots \\ \omega_1^{(n)} & \omega_2^{(n)} & \dots & \omega_n^{(n)} \end{vmatrix}$$

e quello a destra, per la legge di moltiplicazione dei determinanti è

$$|\bar{u}_{rt}| \cdot |a_{ik}| \cdot \begin{vmatrix} \omega_1^{(1)} & \dots & \omega_n^{(1)} \\ \dots & \dots & \dots \\ \omega_1^{(n)} & \dots & \omega_n^{(n)} \end{vmatrix},$$

onde rilevasi

$$N(\alpha)\,|\omega_k^{(s)}| = \bar{X}.\, N(A) \cdot |\omega_k^{(s)}|$$

e siccome $|\omega_k^{(s)}| = \sqrt{\Delta(\omega_1 \omega_2 \dots \omega_n)} = \sqrt{\mathfrak{D}} \neq 0$, ne segue

$$(7) \qquad \bar{X} = \frac{N\alpha}{N(A)},$$

che è la forma (I) dimostrata per valori interi delle x_i.

Pel principio d'identità algebrica, essa è dunque vera in generale.

La forma

$$(8) \qquad X = \sum_{i_1 i_2 i_n} a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \quad (i_1 + i_2 + \dots i_n = n),$$

che abbiamo coordinato all'ideale A, ha coefficienti razionali interi $a_{i_1 i_2 \dots i_n}$, e se per discriminante di una qualunque forma di grado n

$$F = v_1 v_2 \dots v_n$$

decomponibile nel prodotto di n forme lineari $v_1, v_2 \dots v_n$, s'intende il quadrato del determinante delle n forme lineari componenti, vediamo dalla (I) che per la forma X il discriminante è

$$\frac{1}{(NA)^2} \Delta(\alpha_1 \alpha_2 \dots \alpha_n) = \mathfrak{D} \qquad (\S 24)$$

cioè: <u>Il discriminante della forma X eguaglia il numero fondamentale del corpo.</u>

Se diamo alle x_i valori interi h_i, la forma X assume valori interi, che si dicono i numeri rappresentabili dalla forma. Per vedere quali sono questi numeri basta ricorrere alla formola (7) coll'osservare che, essendo α un numero di A, l'ideale principale (α) è divisibile per A, poniamo

$$(\alpha) = A \cdot \mathcal{M},$$

dove $\mathcal{M}$ è un ideale moltiplicatore di A, e quindi di ogni altro della medesima classe. Viceversa, se $\mathcal{M}$ è un moltiplicatore $A\mathcal{M} = (\alpha)$ è un ideale principale ed α è un numero di A. Ora abbiamo

$$\mathcal{N}((\alpha)) = \mathcal{N}(A)\, \mathcal{N}(\mathcal{M}),$$

e siccome

$$\mathcal{N}((\alpha)) = \pm \mathcal{N}\alpha,$$

secondo che la norma $\mathcal{N}\alpha$ del numero α è positiva o negativa, così la (7) acquista semplicemente la forma

$$\bar{X} = \pm \mathcal{N}(\mathcal{M}).$$

Se si ricorda che i moltiplicatori non sono altro che gli ideali della classe inversa di quella a cui A ap-

partiene (§ 33) ne segue:

I numeri rappresentabili dalla forma X (coordinata all'ideale A) sono le norme degli ideali M della classe inversa di A presi col segno positivo se il numero α che genera l'ideale principale $(\alpha) = AM$ ha $N\alpha > 0$ e col segno negativo nel caso contrario.

Al § 28 teorema C), abbiamo dimostrato che l'ideale moltiplicatore M si può sempre scegliere in guisa che sia primo con un ideale prefissato, e di qui deduciamo che $N(M)$ si può rendere primo con un numero razionale intero qualunque k per la qual cosa basterà rendere M primo con (k). E infatti sia m il più piccolo intero contenuto in M, divisore quindi di $N(M)$. Poichè M, (k) sono primi fra loro, sarà $M.(k)$ il minimo multiplo comune, e se indichiamo con d il massimo comun divisore di (m, k), sarà $\frac{mk}{d}$ il minimo multiplo comune di questi due numeri, che dovrà dunque dividere $M.(k)$, essendo $\frac{mk}{d}$ contenuto tanto in M che in (k). Ma poichè k è già contenuto in (k), sarà $\frac{m}{d}$ contenuto in M e quindi, per la nostra ipotesi, $d = 1$, vale a dire m è primo con k. Ma allora anche $N(m) = m^n$ è primo con k, e siccome m è divisibile per

M, è anche N(α) divisibile per N(M), che è dunque un numero primo con l, come si voleva.

Risulta di qui che la forma X può rappresentare numeri primi con qualunque numero prescritto k, e quindi i suoi coefficienti $a_{i_1 i_2 \ldots i_n}$ sono complessivamente primi fra loro, o come si dice: <u>la forma X è primitiva</u>.

Ora dimostriamo che: <u>Eccettuato il caso dei corpi quadratici immaginarii, ogni numero rappresentabile da X ammette infinite rappresentazioni diverse</u>.

Sappiamo infatti che esistono infinite unità e fra queste certamente infinite di norma positiva, eventualmente anche unità di norma negativa (§§ 20-22). Ora se ε è un'unità di norma N(ε) = +1, moltiplicando tutti i numeri α dell'ideale A per ε, si ottengono i numeri stessi in altro ordine e la norma conserva il suo segno. Secondo la formola (7), i due numeri diversi α, εα danno dunque rappresentazioni diverse di ± N(M) per la forma X, ed il segno rimane il medesimo.

Se poi esistono anche unità di norma negativa, allora sono sempre rappresentabili (infinite volte) per la forma X tanto N(M) che −N(M). Quando invece i nu-

meri del corpo hanno tutte le norme positive, come avviene quando il grado n del corpo è pari e tutti i corpi coniugati siano due a due complessi coniugati, allora la forma X rappresenta esclusivamente numeri positivi.

Tutto ciò che abbiamo detto fin qui vale per qualunque ideale A, e se in particolare facciamo coincidere A coll'ideale unità, allora $N(A)=1$, e per la (7) il problema della rappresentazione dei numeri razionali m per la forma X equivale perfettamente all'altro della ricerca dei numeri α del corpo con assegnata norma

$$N\alpha = m.$$

In particolare la ricerca delle unità, compiuta da Dirichlet, equivale alla risoluzione in numeri interi dell'equazione d'analisi indeterminata (razionale)

$$\sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} = \pm 1 \quad (i_1+i_2+\cdots+i_n=n)$$

§ 38

Corrispondenza delle classi di forme X alle classi di ideali.

Moltiplicazione degli ideali e composizione delle forme.

Nel risultato principale ottenuto al paragrafo precedente si vede già che le proprietà della forma decomponibile X non dipendono dalla base $[\alpha_1, \alpha_2, \dots \alpha_n]$ scelta per l'ideale A, ed anzi rimangono essenzialmente invariate cangiando l'ideale A in uno equivalente.

Per esaminare la cosa più da vicino, cominciamo dal ricercare come varia la forma X al variare della base dell'ideale A. Sia $[\beta_1, \beta_2 \dots \beta_n]$ una nuova base di A, ottenuta dall'eseguire sull'antica $[\alpha_1, \alpha_2 \dots \alpha_n]$ una sostituzione lineare

$$(1) \qquad \beta_i = \sum_{k=1}^{k=n} c_{ik}\alpha_k \qquad (i = 1, 2, \dots n)$$

a coefficienti c_{ik} razionali interi e determinante $|c_{ik}| = \pm 1$, e senz'altro supponiamo come è lecito $|c_{ik}| = +1$. Allora se poniamo

$$(2) \qquad \varphi = \sum_i \alpha_i x_i \text{ , in generale } \varphi^{(s)} = \sum_i \alpha_i^{(s)} x_i \text{ ,}$$

la forma X coordinata alla base $[\alpha_1, \alpha_2 \dots \alpha_n]$ è data per la (I) da

$$(a) \qquad X = \frac{1}{N(A)} \cdot \varphi^{(1)} \varphi^{(2)} \dots \varphi^{(n)}.$$

Ed ora indicando con $y_1, y_2 \dots y_n$ nuove variabili poniamo similmente

$$(3) \qquad \psi = \sum_k \beta_k y_k \quad , \qquad \psi^{(s)} = \sum_k \beta_k^{(s)} y_s$$

e sarà

$$(\ddot{5}) \qquad Y = \frac{1}{N(A)} \psi^{(1)} \psi^{(2)} \dots \psi^{(n)}.$$

Ora, avendosi dalle (3), (1)

$$\psi = \sum_i \alpha_i \sum_k c_{ki} y_k ,$$

noi identifichiamo ψ con φ (generalmente $\psi^{(s)}$ con $\varphi^{(s)}$), legando le x, y <u>colla sostituzione unimodulare a coefficienti razionali interi</u>

$$(4) \qquad x_i = \sum_k c_{ki} y_k .$$

Dunque la nuova forma decomponibile Y nasce dall'antica X eseguendo sulle variabili di questa la sostituzione unimodulare (4); e viceversa Y si trasforma in X colla sostituzione unimodulare inversa. Due tali forme X, Y, che nascono l'una dall'altra eseguendo sulle variabili una sostituzione unimodulare a coefficienti razionali interi diconsi <u>equivalenti</u>, essendo manifesto a priori che rappresentano gli stessi numeri. Ma, invertendo le considerazioni precedenti, è anche chiaro che se dalla forma primi-

tiva X si passa ad una equivalente Y, questa ultima è la forma decomponibile corrispondente ad una nuova base dell'ideale.

Vediamo ora quale effetto si produce sulla forma X quando si passa da un ideale A ad un altro $\bar{A}$ della medesima classe (equivalente). In tal caso si possono scegliere le due basi $[\alpha_1, \alpha_2 \cdots \alpha_n]$, $[\bar{\alpha}_1, \bar{\alpha}_2 \cdots \bar{\alpha}_n]$ in modo che siano proporzionali, che si abbia cioè (§ 33)

$$\bar{\alpha}_i = \sigma \alpha_i \qquad (i = 1, 2, \ldots n),$$

essendo σ un numero frazionario del corpo, e noi scriveremo anche

$$\bar{A} = \sigma A.$$

Ma qui conviene restringere la definizione di equivalenza e riguardare come equivalenti i due ideali $\bar{A}, A$ soltanto quando il numero σ ha norma positiva. Con ciò viene anche generalmente cangiata la definizione di classi di ideali, ma i teoremi sulle classi rimangono veri anche colla nuova definizione. Ora se poniamo

$$\varphi = \sum_i \alpha_i x_i \quad , \quad \varphi^{(s)} = \sum_i \alpha_i^{(s)} x_i$$

$$\bar{\varphi} = \sum_i \bar{\alpha}_i x_i = \sigma\varphi, \quad \bar{\varphi}^{(s)} = \sigma^{(s)} \varphi^{(s)}$$

e chiamiamo X la forma corrispondente a φ, ed $\bar{X}$ quella corrispondente a $\bar{\varphi}$, abbiamo per la (I) § precedente

$$X = \frac{1}{N(A)} \varphi^{(1)} \varphi^{(2)} \dots \varphi^{(n)} \quad , \quad \bar{X} = \frac{1}{N(\bar{A})} \bar{\varphi}^{(1)} \bar{\varphi}^{(2)} \dots \bar{\varphi}^{(n)}$$

e siccome per le precedenti

$$\bar{\varphi}^{(1)} \bar{\varphi}^{(2)} \dots \bar{\varphi}^{(n)} = N\sigma . \varphi^{(1)} \varphi^{(2)} \dots \varphi^{(n)}$$

$$N(\bar{A}) = N\sigma . NA \, ,$$

ne risulta $\bar{X} = X$ cioè le due forme coordinate sono identiche.

Ne concludiamo quindi che ad ogni classe di ideali (nel senso ristretto di equivalenza) corrisponde una ed una sola classe di forme decomponibili e alle trasformazioni delle forme di questa classe l'una nell'altra corrisponde il passaggio da una base all'altra dell'ideale. [Se la corrispondenza sia univoca anche in senso inverso non è stato finora deciso].

Fra le trasformazioni della forma X in altre della medesima classe si possono in particolare considerare quelle che <u>trasformano X in sè medesima</u>. Queste costituiscono il così detto gruppo <u>automorfo</u> della X in sè, ed è facile vedere che tale gruppo G con-

tiene in ogni caso (eccetto pei corpi quadratici immaginarii) infinite sostituzioni. Prendasi infatti una qualunque unità ε di norma positiva $N(\varepsilon)=1$, allora insieme alla base

$$[\alpha_1, \alpha_2, \dots \alpha_n]$$

formano una nuova base di A i numeri

$$[\varepsilon\alpha_1, \varepsilon\alpha_2, \dots \varepsilon\alpha_n]$$

perchè $\Delta(\varepsilon\alpha_1, \varepsilon\alpha_2, \dots \varepsilon\alpha_n) = (N(\varepsilon))^2 \Delta(\alpha_1, \alpha_2, \dots \alpha_n) = \Delta(\alpha_1, \alpha_2 \dots \alpha_n)$ (§ 23). Ma allora se poniamo

$$\varphi = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n, \quad \varphi^{(s)} = \alpha_1^{(s)} x_1 + \alpha_2^{(s)} x_2 + \dots + \alpha_n^{(s)} x_n$$

$$\psi = \varepsilon\alpha_1 x_1 + \varepsilon\alpha_2 x_2 + \dots \varepsilon\alpha_n x_n = \varepsilon\varphi, \quad \psi^{(s)} = \varepsilon^{(s)}\varphi^{(s)},$$

si ha manifestamente

$$\varphi^{(1)}\varphi^{(2)} \dots \varphi^{(n)} = \psi^{(1)}\psi^{(2)} \dots \psi^{(n)},$$

e alle due basi $[\alpha_1, \alpha_2 \dots \alpha_n]$, $[\varepsilon\alpha_1, \varepsilon\alpha_2, \dots \varepsilon\alpha_n]$ è dunque coordinata la stessa forma decomponibile X. In tal caso adunque la sostituzione unimodulare (4) cangia la forma X in sè medesima. Facendo percorrere alla ε le infinite unità di norma positiva, si hanno così infinite sostituzioni che trasformano X in sè medesima e costituiscono già per sè un <u>gruppo</u> infinito, contenuto nel gruppo automorfo.

Esaminiamo da ultimo quale significato acquista per le nostre forme decomponibili X la moltiplicazione degli ideali a cui sono associate. Siano

$$A=[\alpha_1, \alpha_2, \dots \alpha_n] \quad , \quad B=[\beta_1, \beta_2 \dots \beta_n]$$

due ideali qualunque e

$$C=AB=[\rho_1, \rho_2, \dots \rho_n]$$

l'ideale loro prodotto. Siccome tutti i numeri $\alpha_i \beta_k$ appartengono all'ideale prodotto, sussistono le relazioni

$$\alpha_i \beta_k = \sum_j p_{ik}^{(j)} \rho_j ,$$

colle $p_{ik}^{(j)}$ numeri interi razionali. Se ora, nei tre sistemi di variabili $(x_i), (y_i), (z_i)$, consideriamo le tre forme lineari

$$\varphi = \sum_i \alpha_i x_i , \quad \psi = \sum_k \beta_k y_k , \quad \chi = \sum_j \rho_j z_j ,$$

dalla relazione precedente risulta subito che, ove le variabili $\underline{z}$ si esprimono per le x, y colla sostituzione <u>bilineare</u>

$$(5) \qquad z_j = \sum_{ik} p_{ik}^{(j)} x_i y_k ,$$

si avrà $\chi = \varphi \psi$, e in generale, passando ai numeri coniugati

$$\varphi^{(s)} \psi^{(s)} = \chi^{(s)} .$$

Ora se poniamo

$$X = \frac{1}{N(A)} \varphi^{(1)}\varphi^{(2)}\dots\varphi^{(n)}, \quad Y = \frac{1}{N(B)} \psi^{(1)}\psi^{(2)}\dots\psi^{(n)}, \quad Z = \frac{1}{N(C)} \chi^{(1)}\chi^{(2)}\dots\chi^{(n)},$$

dalla relazione precedente e dall'essere $N(C) = N(A)\,N(B)$ segue che, legando le z alle x, y colla sostituzione bilineare (5), risulta identicamente

$$Z = X\,Y.$$

Dunque: la forma decomponibile Z, corrispondente al prodotto di due ideali, si risolve, mediante la sostituzione bilineare (5), nel prodotto delle due forme decomponibili corrispondenti agli ideali fattori. Per questo la forma Z si dice composta dalle due X, Y, e vediamo dunque che la moltiplicazione degli ideali corrisponde alla composizione delle forme decomponibili associate.

Per il caso $n = 2$ la composizione delle forme quadratiche binarie venne trattata da Gauss nelle Disquisitiones arithmeticae, anticipando così per questo caso la teoria della moltiplicazione degli ideali.

§ 39.

Confronto dei corpi algebrici. - Corpo di Galois contenente dati corpi algebrici.

Fino ad ora, in questa esposizione delle parti fondamentali dell'aritmetica dei corpi algebrici, il corpo algebrico fondamentale era fisso. Ma si possono ancora confrontare corpi algebrici diversi fra di loro e studiare le eventuali relazioni fra i numeri dell'uno e quelli dell'altro, fra i loro ideali ecc. In questo studio la nozione fondamentale è quella di corpi <u>divisori</u> di un altro corpo (sottocorpi).

Si dice che un corpo algebrico k è divisore di un altro K quando il primo è tutto contenuto nel secondo, il quale a sua volta si dirà <u>multiplo</u> del primo (o sopracorpo). - Senza addentrarci qui in tale studio, ci limiteremo a stabilire un risultato che sta a base della teoria di Galois delle equazioni algebriche e riconduce in sostanza lo studio dei corpi algebrici a quello dei corpi <u>normali</u> o di <u>Galois</u>, come già abbiamo accennato al § 17. Esso

consiste nel teorema:

A) Dato un numero qualunque r di corpi algebrici: $k_1, k_2, \dots k_r$, esiste sempre un corpo K di Galois, di cui $k_1, k_2 \dots k_r$ sono tutti divisori.

Per costruirlo si procederà nel modo seguente: Siano $n_1, n_2 \dots n_r$ i rispettivi gradi di $k_1, k_2 \dots k_r$ e indichiamo con

$$\varphi_1(x) = 0 \quad , \quad \varphi_2(x) = 0 \quad \dots \quad \varphi_r(x) = 0$$

le rispettive equazioni irriducibili di questi gradi à cui soddisfano i numeri fondamentali $\theta_1, \theta_2, \dots \theta_r$ di $k_1, k_2 \dots k_r$ (insieme a tutti i loro coniugati). Poniamo

$$f(x) = \varphi_1(x)\, \varphi_2(x) \dots \varphi_r(x) = 0$$

e consideriamo l'equazione di grado $n = n_1 + n_2 + \dots + n_r$

$$f(x) = 0 ,$$

le cui radici, tutte distinte, indicheremo complessivamente con

$$x_1 , x_2 , \dots x_n ,$$

e comprenderanno tutti e soli i numeri $\theta_1, \theta_2, \dots \theta_r$, insieme ai loro coniugati.

Se ora con $a_1, a_2, \dots a_n$ indichiamo n numeri razio-

nali interi arbitrarii e poniamo

$$(1) \qquad \omega = a_1 x_1 + a_2 x_2 + \dots + a_n x_n ,$$

dimostreremo che questo numero algebrico ω, solo che si evitino per $a_1, a_2, \dots a_n$ sistemi speciali di valori in numero finito, genererà appunto il corpo K di Galois domandato, contenente come divisori i corpi $k_1, k_2 \dots k_r$ (e tutti i loro coniugati).

Per dire subito quali sono gli eventuali valori da evitarsi per i numeri razionali $a_1, a_2 \dots a_n$, consideriamo una qualunque permutazione $(i_1, i_2 \dots i_n)$ degli indici $(1, 2, \dots n)$ e denotiamo con

$$s_i = \begin{bmatrix} x_{i_1} & x_{i_2} & \dots & x_{i_n} \\ x_1 & x_2 & \dots & x_n \end{bmatrix}$$

la sostituzione corrispondente, con ω_{s_i} il numero algebrico che nasce dal fondamentale (1) effettuando sulle x la permutazione s_i. Corrispondentemente alle $N = n!$ sostituzioni, fra le quali figura l'identità, che intenderemo sia la $s_1 = 1$ $(\omega_1 = \omega)$, avremo $N = n!$ di siffatti numeri algebrici

$$(2) \qquad \omega = \omega_{s_1} , \omega_{s_2} , \omega_{s_3} \dots \omega_{s_N} ,$$

e i valori da evitarsi per i coefficienti razionali a_i saranno quelli, in numero finito, pei quali eventual=

mente due dei numeri (1) riuscissero fra loro eguali. Ora eguagliando due di siffatti valori per es. ω_{s_i}, ω_{s_k}, risulterebbe la relazione

$$(3) \qquad a_1(x_{i_1}-x_{k_1})+a_2(x_{i_2}-x_{k_2})+\cdots+a_n(x_{i_n}-x_{k_n})=0,$$

che non è un'identità nelle a, poichè $s_i \neq s_k$. Specializziamo ancora le a_i e poniamo

$$a_1=1,\ a_2=h,\ a_3=h^2,\dots a_n=h^{n-1} \quad (h \text{ razionale});$$

la (3) è per h un'equazione di grado $n-1$ al massimo e, pure ammesso che abbia radici h razionali, queste non potranno essere più di $n-1$. Facendo percorrere dunque agli indici (i,k) le $N_2=\frac{N(N-1)}{2}$ coppie possibili, si avranno al massimo $(n-1)N_2$ valori critici per h, che possiamo sempre intendere evitati.

Ciò posto, ed ammesso che gli N numeri algebrici (3) siano tutti fra loro diseguali, avremo corrispondenza biunivoca fra questi numeri e le N sostituzioni s_i.

Ora dimostriamo che:

B) Qualunque funzione razionale (a coefficienti razionali di $x_1, x_2, \dots x_n$

$$F(x_1, x_2, \cdots x_n)$$

può esprimersi come funzione razionale di $\omega = \omega_{s_1}$, cioè ogni numero algebrico del corpo determinato da $x_1, x_2 \cdots x_n$ appartiene al corpo determinato dal numero algebrico ω (o da qualunque altro ω_{s_i} dei numeri (2)).

Le N sostituzioni $s_1, s_2 \dots s_N$ formano tutte le possibili $n!$, cioè costituiscono il gruppo totale e se le moltiplichiamo tutte, da una stessa parte (per es. a destra) per una di esse poniamo s_i, non faranno che riprodursi in altro ordine. Ne segue che le funzioni simmetriche elementari degli N numeri (2)

$$\omega_{s_1} + \omega_{s_2} + \cdots + \omega_{s_N}$$

$$\omega_{s_1}\omega_{s_2} + \omega_{s_1}\omega_{s_3} + \cdots + \omega_{s_{N-1}}\omega_{s_N}$$

$$\omega_{s_1}\omega_{s_2}\omega_{s_3} + \cdots\cdots$$

$$\omega_{s_1}\omega_{s_2}\cdots\omega_{s_N}$$

risultano funzioni simmetriche di $x_1, x_2 \cdots x_n$ e, come tali, razionalmente esprimibili pei coefficienti della equazione fondamentale $f(x) = 0$, cioè sono numeri razionali. Dunque, nel polinomio di grado n in y

$$(4) \qquad F(y) = (y - \omega_{s_1})(y - \omega_{s_2})\cdots(y - \omega_{s_N}) = y^N + \beta_1 y^{N-1} + \beta_2 y^{N-2} + \cdots + \beta_n,$$

i coefficienti β sono numeri razionali. L'equazione $F(y) = 0$, a coefficienti razionali, le cui radici sono ap-

punto i numeri (2), è quella che prende il nome di <u>risolvente di Galois</u> della proposta $f(x)=0$. Questa risolvente potrà essere irriducibile ovvero riducibile, ma in quest'ultimo caso, come ora vedremo, si decomporrà in fattori irriducibili di egual grado. Per dimostrare il teorema fondamentale B) enunciato, immaginiamo di eseguire sulle x, entro la funzione razionale data F, tutte le possibili sostituzioni s_i e indichiamo con

$$F_{s_1}=F\,,\quad F_{s_2}\,,\ \cdots\ F_{s_N}$$

i valori (numeri algebrici) così ottenuti, fra i quali questa volta potranno anche esservene degli eguali.
Si costruisca il polinomio di grado $N-1$ in y

$$\Psi(y)=\left(\frac{F_{s_1}}{y-\omega_{s_1}}+\frac{F_{s_2}}{y-\omega_{s_2}}+\cdots+\frac{F_{s_N}}{y-\omega_{s_N}}\right)\cdot\Phi(y)=$$

$$=F_{s_1}(y-\omega_{s_2})\cdots(y-\omega_{s_N})+F_{s_2}(y-\omega_{s_1})(y-\omega_{s_3})\cdots$$

$$\cdots(y-\omega_{s_N})+\cdots+F_{s_N}(y-\omega_{s_1})(y-\omega_{s_2})\cdots(y-\omega_{s_{N-1}});$$

vediamo che i suoi coefficienti sono ancora funzioni simmetriche delle x, e per ciò numeri razionali:

$$\Psi(y)=\rho_0\,y^{N-1}+\rho_1\,y^{N-2}+\cdots+\rho_{N-1}\,,$$

colle ρ numeri razionali. Ora, se nella identità

$$(5)\qquad \Psi(y)=\sum_{s_i}\frac{F_{s_i}}{y-\omega_{s_i}}\cdot\Phi(y)$$

poniamo $y = \omega_{s_1}$, ne risulta

$$\Psi(\omega_{s_1}) = F_{s_1}(\omega_{s_1} - \omega_{s_2})(\omega_{s_1} - \omega_{s_3}) \cdots (\omega_{s_1} - \omega_{s_N}),$$

cioè
$$\Psi(\omega) = F(x_1, x_2, \cdots x_n) \cdot \Phi'(\omega),$$

avendo indicato con $\Phi'(y)$ il polinomio derivato di $\Phi(y)$. Così, essendo $\Phi'(\omega) \neq 0$, perchè $\Phi(y) = 0$ non ha radici multiple, ne risulterà la formola

$$(I) \qquad F(x_1, x_2, \cdots x_n) = \frac{\Psi(\omega)}{\Phi'(\omega)};$$

la quale dimostra appunto quanto è asserito nell'enunciato del teorema B). Ma di più osserviamo che se nella identità (5) in luogo di porre $y = \omega_{s_1}$, poniamo $y = \omega_{s_i}$, ne segue similmente

$$(I^*) \qquad F_{s_i} = \frac{\Psi(\omega_{s_i})}{\Phi'(\omega_{s_i})}$$

e questo dimostra che: è lecito nella (I) eseguire a destra e a sinistra una qualunque sostituzione s_i sulle $x_1, x_2 \cdots x_n$ e l'eguaglianza resta verificata.

Se nella formola (I) poniamo successivamente $F = x_1$, $F = x_2$, $\cdots$ $F = x_n$, vediamo che i numeri algebrici $x_1, x_2, \cdots x_n$ appartengono tutti al corpo algebrico K generato dal numero $\underline{\omega}$. Se si fa invece $F = \omega_{s_i}$ si vede che ω_{s_i} appartiene al corpo stesso K, in particolare vi appartengono i coniugati di ω. Il corpo K è dun-

que effettivamente normale, cioè è un corpo di Galois. Così il teorema A) è completamente dimostrato.

Aggiungiamo ora alcune osservazioni complementari. Siccome ω soddisfa già all'equazione $F(y)=0$ di grado $N=n!$, il grado q del corpo K è certo $\leq N$ ed ora facilmente vediamo che è sempre q un divisore di N. Sia infatti $\omega' = \omega_{s_i}$ un'altra qualunque radice di $F(y)=0$ e q' il grado del corpo K' da essa generato. Siccome per la (I) ω' appartiene anche a K, così è $q' \leq q$; ma, per la stessa ragione, anche ω appartiene a K', cioè $q \leq q'$, e quindi $q'=q$, $K'=K$. Dunque le varie radici $\omega_{s_1}, \omega_{s_2} \cdots \omega_{s_N}$ della $F(y)=0$ generano tutte lo stesso corpo K di Galois, al quale appartengono $x_1, x_2 \cdots x_n$, o in altre parole: <u>Se il polinomio $F(y)$ è riducibile, si decompone in fattori tutti di eguàl grado q.</u> Per ciò questo numero q è un divisore di $N=n!$, come sopra è asserito.

Manifestamente il corpo K di Galois, così costruito, è il minimo corpo di Galois a cui appartengono i numeri algebrici $x_1, x_2, \cdots x_n$, e viene individuato da questi.

§ 40.

Relazione col gruppo di Galois per un'equazione $f(x)=0$. Divisori del corpo K e sottogruppi del gruppo.

A questo punto non possiamo tralasciare di dedurre da queste nozioni quella del gruppo di Galois per una data equazione $f(x)=0$ priva di radici multiple che possiamo sempre supporre decomposta nei suoi fattori irriducibili, al modo del § precedente. Supponiamo il corpo K di Galois costruito di grado q (divisore di $n!$), e indichiamo con

$$\Psi(y)$$

il primo fattore irriducibile di grado q della risolvente di Galois $F(y)=0$, sia quello a cui appartengono le radici

$$\omega = \omega_{s_1}, \omega_{s_2} \dots \omega_{s_q}.$$

Dimostriamo: Le q sostituzioni $s_1, s_2 \dots s_q$ formano gruppo fra loro, cioè se s_i, s_k sono due qualunque di esse (diverse od eguali), la sostituzione prodotto $s_i s_k = s_l$ appartiene nuovamente a queste $(l \leq q)$.

Difatti, ω_{s_i} appartenendo al corpo K, la (I) può porsi sotto la forma

$$(6) \qquad \omega_{s_i} = \Theta(\omega) = \Theta(\omega_{s_1})$$

con Θ polinomio razionale intero (a coefficienti razionali) in ω di grado $q-1$ al massimo. Per l'osservazione fatta sopra sulla formola (I^*), in questa relazione (6) è lecito operare a destra e a sinistra una qualunque sostituzione s in particolare la s_k, onde ritevasi

$$\omega_{s_i s_k} = \Theta(\omega_{s_k}) .$$

D'altra parte, siccome il polinomio $\Psi(y)$ si annulla per $y = \omega_{s_i}$, abbiamo

$$\Psi(\Theta(\omega_{s_1})) = 0,$$

cioè il polinomio $\Psi(\Theta(\omega_{s_1}))$ si annulla per la radice ω_{s_1} della equazione irriducibile $\Psi(y) = 0$, indi per tutte le altre, in particolare

$$\Psi(\Theta(\omega_{s_k})) = 0,$$

cioè $\Psi(\omega_{s_i s_k}) = 0$. Dunque $\omega_{s_i s_k}$ è un'altra radice di $\Psi(y)$, sia

$$\omega_{s_i s_k} = \omega_{s_l} ,$$

ed allora $s_i s_k = s_l$, c.d.d.

<u>Il gruppo</u> G_q <u>generato dalle</u> q <u>sostituzioni</u> $s_1 = 1, s_2, \dots$ $\dots s_q$, <u>pienamente determinato dalla equazione</u> $f(x)=0$

(priva di radici multiple) è quello che porta il nome di gruppo di Galois dell'equazione.

Per riconoscere le sue proprietà caratteristiche, basta fondarsi sulle osservazioni seguenti:

1° Se $\Omega = F(x_1\, x_2 \cdots x_n) = \theta(\omega)$ è un qualunque numero algebrico del corpo K, i suoi coniugati sono

$$F_{s_1},\ F_{s_2} \cdots F_{s_q}.$$

Questo risulta immediatamente dalle considerazioni alla fine del § 11.

2° Vi ha identità fra le funzioni razionali (a coefficienti razionali di $x_1\ x_2 \cdots x_n$ e i numeri di K.

Ora un numero algebrico è razionale allora ed allora soltanto che il suo valore coincide con quelli dei suoi coniugati. Pertanto al gruppo G di Galois della $f(x)=0$ appartengono le proprietà caratteristiche seguenti:

I) Ogni funzione razionale (a coefficienti razionali) delle radici $x_1, x_2 \ldots x_n$ della proposta $f(x)=0$, il cui valore numerico non cangia per qualunque sostituzione del gruppo di Galois, è un numero razionale.

II) Se una funzione razionale (a coefficienti razionali) di $x_1, x_2 \dots x_n$ eguaglia un numero razionale, essa rimane numericamente invariata per tutte le sostituzioni del gruppo di Galois.

Queste proprietà caratterizzano in effetto le sostituzioni del gruppo di Galois, poichè se una sostituzione s lascia invariata qualunque funzione razionale delle radici che eguagli un numero razionale, lascierà pure invariata

$$\psi(a) = (a - \omega_{s_1})(a - \omega_{s_2}) \cdots (a - \omega_{s_q})$$

con a razionale qualunque e sarà quindi necessariamente una delle q sostituzioni $s_1, s_2 \dots s_q$.

Ritornando alla composizione della $f(x)$ mediante i suoi fattori irriducibili

$$f(x) = \varphi_1(x)\, \varphi_2(x) \cdots \varphi_r(x),$$

siccome tutti i coniugati di una radice per es. di $\varphi_1(x) = 0$ sono tutte e sole le altre radici dello stesso fattore irriducibile, così è chiaro che il gruppo G di Galois permetterà fra loro esclusivamente le radici di uno stesso fattore irriducibile, ma su queste agirà transitivamente, portando ciascuna radice in qualunque altra.

In particolare tutto questo può applicarsi al caso che la $f(x) = 0$ sia già irriducibile di grado $\underline{n}$, e una sua radice θ individui quindi un corpo algebrico k di grado $\underline{n}$. In tal caso il corpo K di Galois che abbiamo formato è il minimo che sia multiplo di k, e insieme a k contiene naturalmente gli altri suoi coniugati $k', k'' \dots k^{(n-1)}$; il gruppo di Galois in tal caso è transitivo, e $\underline{q}$ è un multiplo di n (§ 11).

Ed ora domandiamo: <u>come si formano tutti gli altri corpi divisori di K?</u>

Sia $\bar{k}$ un tale divisore e $\bar{\theta}$ il suo numero fondamentale, che esprimiamo secondo il § 11 per ω con

$$\bar{\theta} = r(\omega).$$

Se diciamo $\bar{n}$ il grado di $\bar{\theta}$, cioè del corpo $\bar{k}$ divisore, questo è in ogni caso un divisore di q e se poniamo

$$q = r\,\bar{n} \; ; \quad \bar{n} = \frac{q}{r},$$

i coniugati di $\bar{\theta}$ sono r ad r eguali (§ 11). Supponendo che sia

$$\bar{\theta} = \bar{\theta}_{s_1} = \bar{\theta}_{s_2} = \dots = \bar{\theta}_{s_r},$$

le considerazioni già sopra svolte dimostrano che le r sostituzioni

$$s_1, s_2 \dots s_r$$

formano gruppo fra loro (giacchè da $\bar{\theta}_{s_i} = \bar{\theta}_{s_k}$ segue $\bar{\theta}_{s_i s_l} = \bar{\theta}_{s_k s_l}$) che sarà dunque un sottogruppo di G. Così ad ogni divisore $\bar{k}$ di K corrisponde un determinato sottogruppo di G, quello formato dalle sostituzioni di G che lasciano invariato il numero fondamentale $\bar{\theta}$.

Inversamente, se si ha in G_q un qualunque sottogruppo Γ_r, si consideri la totalità dei numeri di K che rimangono invariati per la sostituzione di Γ; questi formano in K un corpo k (divisore) di grado $\frac{q}{r}$.

Queste considerazioni provano la perfetta corrispondenza fra i divisori k del corpo K di Galois e i sottogruppi del gruppo di Galois. Nella teoria algebrica delle equazioni questa è la parte che riguarda la formazione delle diverse <u>risolventi</u>. Nella teoria aritmetica sono invece le relazioni fra i numeri <u>interi</u> del corpo K di Galois e quelli dei suoi divisori k che interessano, in particolare le relazioni fra gli ideali del corpo ambiente e quelli del corpo minore, la loro decomposizione in ideali primi ecc.

Ora Hilbert ha osservato che, per un corpo di Galois,

i teoremi fondamentali dell'aritmetica degli ideali si possono dimostrare molto più facilmente che non nel caso generale di un corpo non normale, e d'altra parte, stabilita questa aritmetica pei corpi di Galois, ne discendono anche le leggi per quella dei loro divisori, cioè in sostanza per qualunque corpo algebrico.

§ 41

Ideali invarianti in un corpo di Galois – Teorema di Hilbert.

Il teorema principale su cui è fondata la teoria degli ideali è quello, dimostrato al § 25 A), dell'esistenza di ideali <u>moltiplicatori</u>. Per i corpi di Galois questo teorema si può dimostrare facilmente col processo seguente di Hilbert. – Se A è un ideale nel corpo K di Galois, anche i suoi coniugati (formati dai numeri coniugati) sono ideali di K stesso; se avviene che A coincida con tutti i suoi coniugati, allora A dicesi un ideale <u>invariante</u> in K. Indichiamo come sopra con q il grado del corpo K di Galois, con $s_1, s_2 \dots s_q$ le sostituzioni del suo gruppo e saranno $A_{s_1}, A_{s_2}, \dots A_{s_q}$ un si-

stema di ideali coniugati, l'ideale A sarà invariante se $A_{s_1} = A_{s_2} = \cdots = A_{s_q}$. Vale ora il:

Teorema di Hilbert - Se A è un ideale invariante, la sua potenza di esponente $Q = q!$ è un ideale principale (d) generato da un numero razionale intero d.

Prendiamo un numero qualunque α di A ed i suoi coniugati

$$\alpha_{s_1}, \alpha_{s_2}, \dots \alpha_{s_q}$$

e consideriamo le loro q funzioni simmetriche elementari $\Sigma \alpha_{s_1}$, $\Sigma \alpha_{s_1} \alpha_{s_2} \cdots$ che saranno q numeri razionali interi $a_1, a_2 \dots a_q$; indichiamo con a l'intero massimo comun divisore dei numeri

$$1) \qquad a_1^{Q}, \; a_2^{\frac{Q}{2}}, \; \dots \; a_q^{\frac{Q}{q}}$$

Così da ciascun numero di A

$$\alpha, \beta, \gamma \dots$$

dedurremo un numero intero razionale corrispondente

$$2) \qquad a, b, c \dots$$

Sia d il massimo comun divisore di tutti i numeri di questa serie 2); proviamo che si ha $A^Q = (d)$. I numeri $\alpha_{s_1}, \alpha_{s_2} \dots \alpha_{s_q}$ appartengono tutti all'ideale A, cioè sono divisibili per A, conseguentemente $a_1 = \Sigma \alpha_{s_1}$

è divisibile per A, $a_2 = \sum \alpha_{s_1}\alpha_{s_2}$ è divisibile per A^2 e così via:

$$a_1 \equiv 0 \pmod{A}\ ,\quad a_2 \equiv 0 \pmod{A^2} \ldots\ a_q \equiv 0 \pmod{A^q};$$

dunque tutti i numeri della serie 1) sono divisibili per A^q, indi anche

$$a \equiv 0 \pmod{A^q}.$$

Lo stesso vale per $b, c \ldots$ e quindi anche pel massimo comun divisore $\underline{d}$ della serie 2) sarà

$$d \equiv 0 \pmod{A^q}.$$

Per ipotesi i numeri

$$\frac{a_1^{\,Q}}{a}\ \frac{a_2^{\,\frac{Q}{2}}}{a}, \ldots\ \frac{a_q^{\,\frac{Q}{q}}}{a}$$

sono tutti interi razionali, e le loro radici Q^{me}

$$\frac{a_1}{a^{\frac{1}{Q}}}\ ,\ \frac{a_2^{\frac{1}{2}}}{a^{\frac{1}{Q}}}, \ldots\ \frac{a_q^{\frac{1}{q}}}{a^{\frac{1}{Q}}}$$

sono quindi interi algebrici, perciò anche i numeri

$$\frac{a_1}{a^{\frac{1}{q}}}\ ,\ \frac{a_2}{a^{\frac{2}{q}}}, \ldots\ \frac{a_q}{a^{\frac{q}{q}}}$$

conseguentemente gli altri

$$\frac{a_1}{d^{\frac{1}{q}}}\ ,\ \frac{a_2}{d^{\frac{2}{q}}}, \ldots\ \frac{a_q}{d^{\frac{q}{q}}}$$

Ma allora se prendiamo l'equazione

$$d\alpha^q - a_1\alpha^{q-1} + a_2\alpha^{q-2} + \cdots \pm a_q = 0,$$

cui soddisfa α, e poniamo

$$\alpha = d^{\frac{1}{q}}\alpha',$$

essa si trasforma per α' nell'altra

$$\alpha'^{q} - \frac{a_1}{d^{\frac{1}{q}}}\alpha'^{q-1} + \frac{a_2}{d^{\frac{2}{q}}}\alpha'^{q-2} + \cdots + \frac{a_q}{d^{\frac{q}{q}}} = 0$$

ed ha coefficienti interi algebrici. Per ciò α' è un intero algebrico, vale a dire ogni numero intero α di A è divisibile per $d^{\frac{1}{q}}$, per ciò ogni numero di A^q per d, il che dimostra essere $A^q \equiv 0 \pmod{d}$. L'ideale A^q e l'ideale principale (d) si dividono dunque l'un l'altro e sono quindi eguali:

$$A^q = (d)$$

secondo l'enunciato.

Dimostrato così il teorema, l'altro della esistenza, per qualsiasi ideale B, di convenienti moltiplicatori M se ne deduce facilmente. Pongasi infatti

$$A = B_{s_1} \cdot B_{s_2} \cdots B_{s_q}$$

e sarà A manifestamente un ideale invariante (perchè $A_{s_i} = B_{s_1 s_i} B_{s_2 s_i} \cdots B_{s_q s_i} = A$). Se questo A è l'ideale **unitario**, allora ponendo

$$M = B_{s_2} \cdots B_{s_q}$$

sarà già M un moltiplicatore di B, avendosi $BM = (1)$.

In ogni caso, siccome $A^a = (d)$, vale a dire

$$B^a B_{s_2}^a \cdots B_{s_q}^a = (d),$$

basterà porre

$$M = B^{a-1} B_{s_2}^a \cdots B_{s_q}^a$$

per avere un moltiplicatore di B.

§ 42

Corpi Abeliani - Corpi circolari - Discriminante e base del corpo circolare alle radici m^{me} dell'unità.

Fra i corpi normali si distinguono quelli il cui gruppo di Galois è formato di sostituzioni due a due permutabili; essi diconsi corpi Abeliani. Se il gruppo G di Galois è formato dalle potenze di una sostituzione fondamentale (gruppo ciclico), il corpo Abeliano si dice corpo ciclico. Si dimostra che i corpi Abeliani si possono comporre con corpi ciclici, e questi, a loro volta, mediante corpi ciclici il cui grado è una potenza di un numero primo.

Le ricerche di Gauss sul problema della divisione del circolo in parti eguali hanno portato al primo e fondamentale esempio di corpi Abeliani che portano

in questo caso il nome di corpi circolari. Sono dunque corpi circolari tutti quelli determinati da una radice m^{ma} primitiva dell'unità (m qualunque), e questo nome di corpi circolari si estende anche a tutti i loro divisori. Tutti questi corpi circolari sono altresì corpi Abeliani, come facilmente si dimostra; ma ricerche più profonde di Kronecker, Weber e Hilbert hanno condotto a riconoscere che inversamente: Ogni corpo Abeliano, nel campo dei numeri razionali, è un corpo circolare.- Noi non possiamo qui entrare nei principii dell'ampia teoria così indicata, ma ci limiteremo alla ricerca fondamentale del corpo circolare più semplice, quello generato dalla radice primitiva m^{ma} dell'unità

$$\varepsilon = e^{\frac{2\pi i}{m}}$$

con m numero primo dispari (Gauss), che chiameremo il corpo $k(\varepsilon)$. Le potenze di ε

$$\varepsilon^0 = 1,\ \varepsilon,\ \varepsilon^2, \dots \varepsilon^{m-1}$$

sono le radici dell'equazione binomia

$$x^m - 1 = 0,$$

e sopprimendo la radice 1, si ha l'equazione

(1) $$f(x) = \frac{x^m - 1}{x-1} = x^{m-1} + x^{m-2} + \dots + x + 1 = 0,$$

a cui ε e le altre radici primitive m^{me} soddisfano. Il grado $\underline{n}$ del corpo $k(\varepsilon)$ non supera certamente $m-1$, cioè $n \leq m-1$, e il provare che si ha precisamente $n = m-1$ equivale a stabilire l'irriducibilità, nel campo razionale, della equazione (1). Questo discende facilmente come caso particolare da un criterio di Eisenstein che fa conoscere una classe di equazioni irriducibili; ma qui conviene meglio stabilire l'irriducibilità della (1) come conseguenza dei teoremi generali sui numeri algebrici. Per questo si osservi che dalla (1) segue l'identità

$$f(x) = (x-\varepsilon)(x-\varepsilon^2)\cdots(x-\varepsilon^{m-1}),$$

nella quale ponendo $x = 1$, risulta

(2) $$m = (1-\varepsilon)(1-\varepsilon^2)\cdots(1-\varepsilon^{m-1}).$$

Così il numero primo razionale $\underline{m}$ appare decomposto, nel corpo $k(\varepsilon)$, negli $m-1$ fattori

$$1-\varepsilon,\ 1-\varepsilon^2, \dots\ 1-\varepsilon^{m-1};$$

però questi, come facilmente dimostriamo, non sono essenzialmente distinti anzi sono tutti associati, differendo dal primo $1-\varepsilon$ soltanto per un fattore unità. Per vederlo si ricordi che l'eguaglianza di due potenze di

due potenze di ε si traduce nella congruenza dei loro esponenti (mod m), e ad ogni esponente r si associ l'altro s determinato da $rs \equiv 1$ (mod m). Il numero

$$\frac{1-\varepsilon^r}{1-\varepsilon} = 1+\varepsilon+\varepsilon^2+\dots+\varepsilon^{r-1}$$

è intero, ma nello stesso tempo è intero anche il suo inverso

$$\frac{1-\varepsilon}{1-\varepsilon^r} = \frac{1-\varepsilon^{rs}}{1-\varepsilon^r} = 1+\varepsilon^r+\varepsilon^{2r}+\dots+\varepsilon^{(s-1)r},$$

e perciò $\frac{1-\varepsilon^r}{1-\varepsilon}$ è un'unità, poniamo

$$\eta_r = \frac{1-\varepsilon^r}{1-\varepsilon}.$$

Così tutti gli $m-1$ fattori a destra in (2) sono numeri associati e la formola stessa si scrive

$$m = \eta_2\eta_3\cdots\eta_{m-1}(1-\varepsilon)^{m-1}.$$

Ponendo

$$(3) \qquad \mu = 1-\varepsilon,$$

vediamo dunque che l'ideale principale (m) è la potenza $(m-1)^{ma}$ dell'ideale principale (μ)

$$(I) \qquad (m) = (\mu)^{m-1},$$

e da questa deduciamo facilmente che (μ) è un ideale <u>primo</u>, ed il grado n del corpo è precisamente $= m-1$ (la equazione (1) è irriducibile). Prendendo infatti le norme nella (I) risulta

$$N(m) = m^n = (N\mu)^{m-1}$$

e poichè m è primo sarà $N(\mu)$ stessa una potenza di m, diciamo m^k, e allora

$$n = k(m-1).$$

Ma siccome n non può superare $m-1$, se ne deduce $n = m-1$ c.d.d., e

$$N(\mu) = m;$$

da questa ultima segue che (μ) è un ideale primo, poichè già la sua norma è il numero primo m. Dalla (I) segue intanto:

A) Il numero primo m è la potenza $(m-1)^{ma}$ dell'ideale primo (μ) $(\mu = 1-\varepsilon)$.

Ed ora procediamo alla determinazione della base pei numeri interi del corpo circolare $k(\varepsilon)$. Per questo cominciamo dal calcolare il discriminante degli $m-1$ interi

$$1, \varepsilon, \varepsilon^2, \dots \varepsilon^{m-2},$$

che sono certamente indipendenti, a causa della irriducibilità della (1), o ciò che è lo stesso quello dei numeri stessi moltiplicati per ε.

$$\Delta(\varepsilon, \varepsilon^2 \cdots \varepsilon^{m-1}) = (N(\varepsilon))^2 \Delta(1, \varepsilon, \varepsilon^2 \dots \varepsilon^{m-1}) = \Delta(1, \varepsilon, \varepsilon^2 \cdots \varepsilon^{m-1}).$$

Il discriminante $\Delta(\varepsilon, \varepsilon^2, \cdots \varepsilon^{m-1})$ è il quadrato del determinante di Vandermonde delle radici della (1) (il discriminante della (1)), dal quale il quadrato del determinante di Vandermonde per le <u>m</u> radici

$$1, \varepsilon, \varepsilon^2, \dots \varepsilon^{m-1}$$

della equazione binomia $x^m - 1 = 0$ (discriminante di questa) differisce solo pel fattore

$$\Pi (1-\varepsilon)^2 (1-\varepsilon^2)^2 \cdots (1-\varepsilon^{m-1})^2 = m^2 \quad \text{(secondo la (2))}$$

Dunque abbiamo

$$\Delta(1, \varepsilon, \varepsilon^2, \cdots \varepsilon^{m-1}) = \frac{1}{m^2} \begin{vmatrix} 1 & \varepsilon & \varepsilon^2 & \dots & \varepsilon^{m-1} \\ 1 & \varepsilon^2 & \varepsilon^{2 \cdot 2} & \dots & \varepsilon^{2(m-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \varepsilon^{m-1} & \varepsilon^{(m-1)^2 2} & \dots & \varepsilon^{(m-1)(m-1)} \end{vmatrix}$$

ed eseguendo il quadrato del determinante a destra per linee osservando che in generale

$$1 + \varepsilon^{r+s} + \varepsilon^{2(r+s)} + \dots + \varepsilon^{(m-1)(r+s)} = \begin{cases} m & \text{se } r+s \equiv 0 \pmod m \\ 0 & \text{se } r+s \not\equiv 0 \pmod m \end{cases}$$

otteniamo

$$\Delta(1, \varepsilon, \varepsilon^2, \cdots \varepsilon^{m-1}) = \frac{1}{m^2} \begin{vmatrix} 0 & 0 & \dots & 0 & m \\ 0 & 0 & & m & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ m & 0 & & 0 & 0 \end{vmatrix},$$

cioè

$$(II) \qquad \Delta(1, \varepsilon, \varepsilon^2, \dots \varepsilon^{m-2}) = (-1)^{\frac{m-1}{2}} m^{m-2}$$

Ottenuto così il valore di questo discriminante, facilmente dimostriamo:

B) <u>Dei numeri interi del corpo $k(\varepsilon)$ una base è costituita appunto dai numeri</u>

$$1, \varepsilon, \varepsilon^2, \dots \varepsilon^{m-2}$$

<u>(ovvero anche da $\varepsilon, \varepsilon^2, \dots \varepsilon^{m-1}$).</u>

Difatti sia $(\omega_1, \omega_2, \dots \omega_{m-1})$ una base di $k(\varepsilon)$ e sia

$$(4) \qquad \varepsilon^i = \sum_{r=1}^{r=m-1} c_{ir} \omega_r \qquad (i = 1, 2 \dots m-1)$$

la sostituzione lineare a coefficienti interi c_{ir} che fa passare dalla base $(\omega_1, \dots \omega_{m-1})$ agli $m-1$ numeri $\varepsilon, \varepsilon^2, \dots \varepsilon^{m-1}$; e indichiamo con $\underline{a}$ il valore del determinante (c_{ir}); avremo (§ 12)

$$\Delta(\varepsilon, \varepsilon^2 \dots \varepsilon^{m-1}) = a^2 \Delta(\omega_1, \omega_2 \dots \omega_{m-1}) = a^2 . D,$$

dove D è il numero fondamentale del corpo $k(\varepsilon)$. Per la (II) questa si scrive

$$(-1)^{\frac{m-1}{2}} m^{m-2} = a^2 . D,$$

onde risulta che il numero razionale intero $\underline{a}$ (e D stesso) non possono avere altri fattori primi all'infuori di $\underline{m}$.

Poniamo che sia

(5) $\quad a = m^r, \quad$ con $2r < m-2$

e dimostriamo che si ha necessariamente $r=0$, ciò che dimostrerà il teorema B).

Se risolviamo le (4) rispetto ai numeri $\underline{\omega}$ della base, e badiamo alle (5), ne deduciamo intanto che ogni intero di $k(\varepsilon)$ ha la forma

$$\alpha = \frac{h_1 + h_2\varepsilon + h_3\varepsilon^2 + \dots + h_{m-1}\varepsilon^{m-2}}{m^r} \qquad \left(r \leq \frac{m-3}{2}\right)$$

dove $h_1, h_2, \dots h_{m-1}$ sono razionali interi, del resto qualunque. Ora se fosse $r>0$ il numero

$$m^r\alpha = h_1 + h_2\varepsilon + h_3\varepsilon^2 + h_{m-1}\varepsilon^{m-2}$$

sarebbe divisibile per $\underline{m}$, per qualunque sistema di valori razionali interi delle h. E siccome per la (I) $(m)=(\mu)^{m-1}$, con $\mu = 1-\varepsilon$, il numero

$$h_1 + h_2(1-\mu) + h_3(1-\mu)^2 + \dots + h_{m-1}(1-\mu)^{m-2}$$

sarebbe sempre divisibile per μ, e quindi, trascurando i multipli di μ, anche il numero razionale intero arbitrario $h_1 + h_2 + \dots h_{m-1}$ sarebbe divisibile per μ, ciò che è assurdo. Se ne conclude che $r=0$, e tutti gli interi di $k(\varepsilon)$ hanno la forma

$$\alpha = h_1 + h_2\varepsilon + h_3\varepsilon^2 + \dots + h_{m-1}\varepsilon^{m-2} \quad \text{(colle } h \text{ razionali interi).}$$

Segue inoltre: Il numero fondamentale D del corpo

$k(\varepsilon)$ è dato da

$$\mathfrak{D} = (-1)^{\frac{m-1}{2}} m^{m-2}.$$

§ 43

Gli ideali primi nel corpo circolare $k(\varepsilon)$ secondo Kummer.

Il corpo circolare $k(\varepsilon)$ coincide manifestamente con tutti i suoi coniugati, ed è per ciò un corpo normale (di Galois); anzi di più esso è ciclico, come ora facilmente dimostriamo. Per questo ordiniamo i numeri della sua base

$$\varepsilon, \varepsilon^2, \ldots \varepsilon^{m-1}$$

in altro modo più opportuno come segue. Indichiamo con g una radice primitiva (mod m), talchè le $m-1$ potenze di g

$$g^0 = 1, g, g^2, \ldots g^{m-2}$$

danno tutti i numeri, non divisibili per m, incongrui (mod m), e ordiniamo i numeri della base nella sua nuova forma

$$(\varepsilon, \varepsilon^g, \varepsilon^{g^2}, \ldots \varepsilon^{g^{m-2}}).$$

Se si cambia ε nel numero coniugato ε^g, questi numeri della base subiscono la sostituzione circolare d'ordi-

ne $m-1$

$$S = (\varepsilon, \varepsilon^{g}, \varepsilon^{g^2} \dots \varepsilon^{g^{m-2}})$$

che appartiene al gruppo di Galois del corpo $k(\varepsilon)$ (§ 40) e colle sue potenze dà tutto il gruppo. Questo è dunque un gruppo ciclico.

Come abbiamo fatto al § 32 pel caso dei corpi quadratici, cerchiamo anche qui, pel campo circolare $k(\varepsilon)$, di determinare i suoi ideali primi P, per la qual cosa dovremo ricercare come si risolvono i numeri primi ordinari p, considerati quali ideali principali, nei loro fattori ideali primi. Pel numero primo m, che è l'unico il quale entri nel numero fondamentale D, la questione è risoluta dalla formola (I) del § precedente, che ne dimostra il comportamento come numero primo critico.

Per ogni altro numero primo $p \neq m$ (non escluso il numero 2) poniamo a base della ricerca le considerazioni seguenti. Se ω è un qualunque intero di $k(\varepsilon)$, dunque della forma

$$\omega = h_1 \varepsilon + h_2 \varepsilon^2 + \dots + h_{m-1} \varepsilon^{m-1} \quad (h_i \text{ interi razionali}),$$

elevando alla potenza p col teorema polinomiale e

trascurando i multipli di p, abbiamo

$$\omega^p \equiv h_1^p \varepsilon^p + h_2^p \varepsilon^{2p} + \dots + h_{m-1}^p \varepsilon^{(m-1)p} \pmod p,$$

cioè pel teorema di Fermat

$$\omega^p \equiv h_1 \varepsilon^p + h_2 \varepsilon^{2p} + \dots + h_{m-1} \varepsilon^{(m-1)p} \pmod p.$$

Ed elevando nuovamente alla potenza p, avremo similmente

$$\omega^{p^2} \equiv h_1 \varepsilon^{p^2} + h_2 \varepsilon^{2p^2} + \dots + h_{m-1} \varepsilon^{(m-1)p^2} \pmod p,$$

e così di seguito. Se supponiamo dunque che il numero primo p appartenga, rispetto al modulo m, all'esponente f, avendosi $p^f \equiv 1 \pmod m$, ne dedurremo

$$\omega^{p^f} \equiv h_1 \varepsilon + h_2 \varepsilon^2 + \dots + h_{m-1} \varepsilon^{m-1} \pmod p,$$

cioè: Se il numero primo p appartiene all'esponente $f \pmod m$, qualunque intero ω di $k(\varepsilon)$ soddisfa alla congruenza

$$\text{(III)} \qquad \omega^{p^f} \equiv \omega \pmod p.$$

Supponiamo ora che sia P uno degli ideali primi in cui si risolve l'ideale principale (p), e cominciamo dal dedurre dalla (III) questa conseguenza importante che: P non può entrare in (p) a potenza maggiore della prima. Se avviene il contrario, poniamo $(p) = P^2 A$, possiamo prendere un intero ω di $k(\varepsilon)$ che sia divisibile

per PQ, ma non per P^2Q, cioè non per p. In tal caso ω^2 è divisibile per P^2Q^2, indi per p; per ciò anche $\omega^{p^f} = \omega^2 \cdot \omega^{p^f - 2}$ è divisibile per p; ma questo contraddice alla (III) perchè ne risulterebbe anche ω divisibile per p. Intanto vediamo che: Se p è un numero primo diverso da m (se non entra nel discriminante), l'ideale principale (p) si risolve in ideali primi tutti fra loro diversi. Questo contegno dei numeri primi non critici è affatto analogo a quello che abbiamo riscontrato al § 32 nel caso dei corpi quadratici e non è che un caso particolare di una proprietà che si verifica per tutti i corpi algebrici e qui dobbiamo limitarci a citare: Il numero fondamentale D di un qualunque corpo algebrico si compone di tutti e soli quei numeri primi ordinarii che sono divisibili pel quadrato di un ideale primo.

Ma ritorniamo al nostro caso particolare, della risoluzione in ideali primi nel corpo circolare $k(\varepsilon)$ dell'ideale principale (p), e dimostriamo: L'esponente f cui appartiene p (mod m) è precisamente il grado di ciascuno degli ideali primi nei quali p si risolve.

Sia f il grado di un tale ideale primo P, onde $N(P) = p^f$.

Sussistendo per qualunque intero ω del corpo la congruenza (III), sussiste a più forte ragione (mod P), cioè la congruenza

$$x^{p^f} - x \equiv 0 \pmod{P}$$

di grado p^f possiede $N(P) = p^{f'}$ radici, e poichè il modulo P è primo si ha dunque necessariamente (§ 31)

$$p^f \geq p^{f'}, \quad f \geq f'.$$

D'altra parte, a causa del teorema di Fermat generalizzato (§ 30), si ha

$$\varepsilon^{p^{f'}-1} \equiv 1 \pmod{P},$$

vale a dire il numero $1-\varepsilon^{p^{f'}-1}$ è divisibile per P. Ora se fosse $p^{f'}-1 \not\equiv 0 \pmod{m}$ questo intero sarebbe un associato di μ (§ 42) e non ammetterebbe altro divisore all'infuori di $(\mu) \neq (P)$; dunque necessariamente

$$p^{f'} \equiv 1 \pmod{m},$$

e per ciò f', come multiplo del minimo f, risulta $\geq f$.
Se ne conclude $f' = f$ ed il risultato finale (di Kummer):
<u>Se il numero primo p è diverso da m, ed appartiene all'esponente f (mod m), talchè $m-1$ si risolve nel prodotto dei due fattori $m-1 = ef$, l'ideale principale (p) si decompone, nel corpo circolare $k(\varepsilon)$, nel prodotto</u>

<u>di e ideali primi diversi</u>

$$(p) = P_1 P_2 \dots P_e ,$$

<u>ciascuno dei quali ha il grado f.</u>

È ben noto che, dato un divisore qualunque f di $m-1$, tra i numeri

$$1, 2, 3, \dots m-1$$

ve ne sono precisamente $\varphi(f)$ che appartengono all'esponente f; per ciò i numeri primi p che si risolvono, in $k(\varepsilon)$, in $e = \frac{m-1}{f}$ ideali primi di grado f sono distribuiti in $\varphi(f)$ progressioni aritmetiche, che hanno per ragione p e per termini iniziali appunto quei $\varphi(f)$ numeri. In virtù di un teorema dimostrato la prima volta da Dirichlet coi mezzi dell'aritmetica analitica, ciascuna di queste progressioni aritmetiche contiene in effetto infiniti numeri primi.

Si osservino i casi estremi $f=1$, $f=m-1$. Nel primo caso i numeri primi p corrispondenti sono quelli $\equiv 1 \pmod{m}$ (della progressione aritmetica $mx+1$) e per ciascuno di essi l'ideale principale (p) si risolve in $m-1$ ideali primi tutti di 1° grado:

$$(p) = P_1 P_2 \dots P_{m-1} .$$

Nell'altro caso $f = m-1$ il numero p è una radice primitiva g del modulo $\underline{m}$ e l'ideale principale (p) è già primo (di grado $m-1$)

$$(p) = P.$$

Se applichiamo p.e. questi risultati generali al caso $n = 3$ del corpo $k(\varepsilon)$ della radice cubica dell'unità, questo coincide col corpo quadratico di Jacobi-Eisenstein per $d = -3$ e ritorniamo a casi particolari delle decomposizioni esaminate al § 32. I numeri primi p che si risolvono in due ideali primi di 1° grado sono quelli $\equiv 1 \pmod 3$, cioè della forma $6n+1$, gli altri che dànno un solo ideale primo di 2° grado sono quelli $\equiv 2 \pmod 3$, cioè il numero primo $\underline{2}$ e quelli dispari della forma $6n-1$.

Capitolo III°

Principii d'aritmetica analitica - La funzione $\zeta(s)$ di Riemann e la funzione generalizzata $\zeta_K(s)$ di Dedekind per un corpo algebrico K -- Formola di Dedekind pel numero h delle classi - Casi del corpo quadratico e del corpo circolare. - Prolungamento analitico della funzione $\zeta(s)$ di Riemann a tutto il piano complesso - Cenno delle recenti ricerche di Hecke sulle proprietà analoghe dalla $\zeta_K(s)$.

§ 44

Algoritmo dei prodotti infiniti - Prime trasformazioni d'Eulero - Divergenza della serie $\Sigma \frac{1}{p}$.

Nelle ricerche di teoria dei numeri esposte nei Capitoli precedenti ci siamo valsi esclusivamente di mezzi aritmetici ed algebrici. Ora andiamo a cominciare lo studio, limitato alle parti fondamentali, di un altro importante ramo della teoria dei numeri, della così detta <u>aritmetica analitica</u>, nella quale si applicano i metodi dell'analisi algebrica

infinita, dell'analisi infinitesimale e della teoria delle funzioni allo studio di proprietà aritmetiche più riposte, che difficilmente sarebbero accessibili ai metodi elementari.

I primi germi dell'aritmetica analitica si riscontrano nella: Introductio in analysin infinitorum di Eulero; ma il loro sviluppo è dovuto principalmente a Dirichlet, che raggiunse per questa via nuovi ed importantissimi risultati.

A base di questi metodi dell'aritmetica analitica stanno alcune formole di conversione di prodotti infiniti in serie (dei quali poi tanti notevoli esempî offri la teoria delle funzioni ellittiche) ed in tutti questi sviluppi conviene tener sempre presenti, per i diversi algoritmi, le nozioni di convergenza, convergenza incondizionata, convergenza assoluta, in fine della convergenza uniforme, quando i termini della serie, o i fattori del prodotto infinito, sono funzioni di una o più variabili, reali o complesse.

Per ricorrervi in seguito, quando occorra, ricordiamo qui tali nozioni fondamentali per l'algoritmo,

meno frequentemente usato, dei prodotti infiniti. Data una serie infinita di quantità, reali o complesse

$$u_1, u_2, \dots u_n \dots,$$

si formi la successione di prodotti

$$P_n = (1+u_1)(1+u_2)\dots(1+u_n) \quad \text{per} \quad n = 1, 2, 3, \dots;$$

se questa successione, per <u>n</u> crescente all'infinito, ha un limite determinato, finito e diverso da zero

$$\lim_{n\to\infty} P_n = P \neq 0,$$

allora si dice che il prodotto infinito $\prod_1^\infty (1+u_n)$ è <u>convergente</u> ed ha per valore P. Noi escludiamo il caso di $P=0$ (come avverrebbe in particolare se uno dei fattori $1+u_n$ si annullasse) perchè in questo caso non tutti i teoremi relativi al caso di convergenza propria restano validi.

Come per ogni successione, la questione dell'esistenza del limite si riporta a quella della convergenza della serie

$$P_1 + (P_2 - P_1) + (P_3 - P_2) + \dots + (P_n - P_{n-1}) + \dots,$$

ovvero, posto

$$v_1 = 1 + u_1 \;, \quad v_n = P_n - P_{n-1} = (1+u_1)(1+u_2)\cdots(1+u_{n-1})\,u_n,$$

della serie $\sum_1^\infty v_n$, e a riconoscere <u>se la sua somma P</u>

è diversa da zero.

Come prima condizione necessaria, per la convergenza del prodotto infinito $\prod(1+u_n)$, si ha questa che esista e sia nullo $\lim_{n=\infty} u_n$. Un primo ed elementare caso è quello in cui tutte le quantità u_n siano reali e positive; allora si ha

a) condizione necessaria e sufficiente per la convergenza del prodotto infinito $\prod_1^\infty (1+u_n)$, se le u_n sono reali e positive, è la convergenza della serie $\sum u_n$.

Supponiamo ora le u_n complesse qualunque, e basterà in tal caso ricorrere alla seguente proprietà che dà una condizione sufficiente (non necessaria) per la convergenza del prodotto infinito:

b) Se la serie dei moduli delle u_n è convergente, è anche convergente il prodotto infinito.

In questa ipotesi (convergenza di $\sum|u_n|$, o convergenza assoluta di $\sum u_n$) la serie $\sum v_n$, associata al prodotto infinito, è convergente assolutamente e si dice perciò che il prodotto infinito converge assolutamente.

Sempre nelle ipotesi precedenti (convergenza di $\sum|u_n|$), si ha:

c) Il prodotto infinito $\prod_1^{\infty}(1+u_n)$ è convergente incondizionatamente (come la serie $\Sigma\, v_n$), cioè alterando comunque l'ordine dei fattori, esso resta convergente e conserva lo stesso valore.

Siano ora le u_n funzioni continue, reali o complesse, di quante si vogliano variabili $x_1, x_2 \dots x_r$ reali o complesse; si dirà che il prodotto infinito $\prod_1^{\infty}(1+u_n)$ è convergente uniformemente in un certo campo chiuso per queste variabili se converge uniformemente la corrispondente serie $\sum v_n$, chè allora, data una quantità ε positiva arbitraria, potremo prendere un indice m tanto grande che si abbia sempre

$$|P_n - P| < \varepsilon \qquad \text{quando } n \geq m,$$

e variando comunque le variabili $x_1, x_2 \dots x_r$ nel campo assegnato. Qui abbiamo la proprietà:

d) Se converge uniformemente la serie $\Sigma\,|u_n|$, converge anche uniformemente il prodotto infinito $\prod_1^{\infty}(1+u_n)$.

Nel seguito, con n indicheremo un intero variabile che percorre tutta la serie dei numeri interi positivi, con p invece un numero primo variabile, che percorre tutta la serie dei numeri primi: 2, 3, 5, 7, 11, ...

Sia ora $f(n)$ una funzione numerica, reale o complessa, dell'indice n, che per due valori arbitrarii n, n' dell'argomento soddisfi all'equazione funzionale

$$(A) \qquad f(n)\,f(n') = f(n\,n')$$

e conseguentemente (affinchè $f(n)$ non sia sempre nulla) all'altra $f(1)=1$; supponiamo inoltre soddisfatta l'altra condizione:

(B) la serie $\sum\limits_n |f(n)|$ sia convergente.

Sotto queste ipotesi, dimostriamo che vale la seguente formola di trasformazione di una serie in prodotto infinito (Eulero)

$$(I) \qquad \sum_n f(n) = \prod_p \frac{1}{1-f(p)},$$

dove s'intende che, nella serie a sinistra, n percorre tutta la serie 1, 2, 3, ... e a destra, nel prodotto infinito p percorre la serie dei numeri primi. Trattandosi poi di convergenza assoluta, indi incondizionata, l'ordine dei termini nella serie, e dei fattori nel prodotto infinito, sarà indifferente.

Cominciamo dall'osservare che, in virtù delle nostre ipotesi, è certamente $|f(n)|<1$ per $n>1$, perchè la serie

$$|f(1)|+|f(n)|+|f(n^2)|+\cdots+|f(n^r)|+\cdots,$$

che è una parte della serie (B), è convergente, e d'altronde, per la supposta proprietà (A), essa è la progressione geometrica

$$1 + q + q^2 + \cdots + q^r + \cdots \quad ; \quad \text{con } q = |f(n)|.$$

Intanto, nel prodotto infinito a destra in (I), è dunque sempre $f(p) \neq 1$ e il prodotto stesso ha un significato ed è convergente assolutamente in senso proprio (diverso da zero), come si vede applicando il criterio b) e c) col porre $u_p = \frac{f(p)}{1-f(p)}$; poichè, essendo convergente la serie $\sum_p |f(p)|$, è pure convergente $\sum_p \frac{|f(p)|}{|1-f(p)|}$, minorante rispetto alla serie $\sum_p \frac{|f(p)|}{1-(f(p))}$.

Ora ogni singolo fattore $\frac{1}{1-f(p)}$, essendo $|f(p)| < 1$, si sviluppa nella progressione geometrica convergente

$$1 + f(p) + (f(p))^2 + (f(p))^3 + \cdots ,$$

cioè per la proprietà (A)

$$(1) \qquad \frac{1}{1-f(p)} = 1 + f(p) + f(p^2) + f(p^3) + \cdots$$

Se pensiamo nel prodotto infinito $P = \prod_p \frac{1}{1-f(p)}$ ordinati i fattori, p.e. nella successione naturale dei numeri primi, e facciamo il prodotto P_n dei primi $\underline{n}$ fattori

$$P_n = \frac{1}{1-f(p_1)} \cdot \frac{1}{1-f(p_2)} \cdots \frac{1}{1-f(p_n)} ,$$

possiamo sviluppare ciascun fattore nella corrispondente

te serie (1) e moltiplicare quindi queste n serie <u>assoluta-mente convergenti</u> fra loro, colla nota regola. Conformemente alla proprietà (A), troviamo subito per P_n lo sviluppo seguente:

$$(2) \qquad P_n = \sum_N f(N),$$

dove N percorre tutti e soli gli interi positivi che si compongono esclusivamente cogli n primi numeri primi: $p_1, p_2 \cdots p_n$. Da questa formola (2) si otterrà ora, con passaggio al limite per $n = \infty$, la (I), argomentando come segue. Se m è un intero positivo, grande a piacere, possiamo poi prendere n tanto grande che tutti i numeri primi $< m$ figurino fra $p_1, p_2 \cdots p_n$. Allora la serie a destra in (2)

$$\sum_N f(N)$$

contiene tutti quei termini della serie $\sum_r f(r)$ in cui $r < m$, insieme ancora ad infiniti altri nei quali però $r \geq m$. Dunque la serie

$$(3) \qquad \sum_r f(r) - \sum_N f(N)$$

contiene termini della serie $\sum f(r)$ che sono tutti al di là di $f(m)$, e quindi, per m sufficientemente grande, la differenza (3) ha un modulo piccolo a piacere. Abbiamo

dunque

$$P = \lim_{n\to\infty} P_n = \lim_{n\to\infty} \sum f(N) = \sum_1 f(r)\,,$$

ciò che dimostra appunto la formola (I).

Una seconda formola importante si ottiene dalla (I), passando dai numeri ai loro logaritmi neperiani, ove si ricordi che per $|z|<1$ si ha

$$\log\left(\frac{1}{1-z}\right) = z + \frac{z^2}{2} + \frac{z^3}{3} + \cdots\,,$$

intendendo che il valore del logaritmo è il <u>principale</u>, cioè quello coll'argomento nell'intervallo $(-\frac{\pi}{2}, +\frac{\pi}{2})$. Prendendo adunque i logaritmi nella (I), risulta dapprima

$$\log \sum_n f(n) = \sum_p \left\{ f(p) + \frac{1}{2} f(p^2) + \frac{1}{3} f(p^3) + \cdots \right\},$$

e la serie a destra si può riguardare come una serie doppia incondizionatamente convergente. Per ciò si può anche scrivere

$$(II) \qquad \log \sum_n f(n) = \sum_p f(p) + \frac{1}{2} \sum_p f(p^2) + \frac{1}{3} \sum_p f(p^3) + \cdots\,,$$

e questa è la seconda formola (d'Eulero) che volevamo stabilire.

È importante poi osservare che queste formole (I) e (II), pel modo stesso come le abbiamo dedotte, valgono anche se la funzione $f(n)$ si suppone <u>nulla</u> tutte le volte

che $\underline{n}$ non è primo con un numero fisso a piacere $\underline{k}$, purchè valga la (A) <u>per n, n' primi con k</u>, e la serie $\Sigma|f(n)|$ sia convergente.

Le considerazioni fondamentali sopra svolte, per la dimostrazione della formola (I), possono anche applicarsi in casi in cui tutte le condizioni supposte non sono soddisfatte; così al caso in cui si prenda $f(n) = \frac{1}{n}$, chè allora è bensi soddisfatta la (A), ma la serie (armonica) $\Sigma \frac{1}{n}$ è divergente. Se ne trae facilmente questa conseguenza:

<u>La serie delle inverse dei numeri primi</u> $\Sigma \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots$ <u>è divergente</u>, ciò che include il teorema dimostrato da Euclide della infinità dei numeri primi. Intanto, per qualunque numero primo $\underline{p}$, vale la trasformazione

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \dots + \frac{1}{p^r} + \dots,$$

e per ciò se vi fosse un numero limitato $\underline{n}$ di numeri primi $p_1, p_2, \dots p_n$ ne trarremmo come sopra

$$(4) \qquad \prod_{i=1}^{i=n} \frac{1}{1-\frac{1}{p}} = \sum_N \frac{1}{N},$$

dove $\underline{N}$ percorrerebbe ora <u>tutti</u> i numeri interi, ciò che è in contraddizione col fatto che la serie armo-

nica è divergente. Ma ora se la serie $\Sigma \frac{1}{p}$ fosse convergente, sarebbe pur convergente in senso proprio per b), cioè diverso da zero, il prodotto $P = \prod_p \left(1 - \frac{1}{p}\right)$, per la (4) convergerebbe la serie delle inverse $\frac{1}{N}$ dei numeri N composti soltanto dei primi $\underline{n}$ numeri primi, onde avremo, per qualunque $\underline{n}$

$$(5) \qquad \Sigma \frac{1}{N} < \frac{1}{P}.$$

Al contrario, essendo divergente la serie armonica $\Sigma \frac{1}{n}$, possiamo prendere $\underline{m}$ tanto grande che sia

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m} > \frac{1}{P}$$

e questo è in contraddizione colla (5), ove per $p_1, p_2 \cdots \cdots p_n$ si prendono i numeri primi $\leq m$.

§ 45

Prima definizione della funzione $\zeta(s)$ di Riemann nel semipiano $\sigma = R(s) > 1$ $(s = \sigma + i\tau)$ - Serie di Dirichlet.

Nella formola (I) d'Eulero del § precedente poniamo

$$f(n) = n^{-s} = e^{-s \log n},$$

dove $\underline{s}$ è una variabile complessa $s = \sigma + i\tau$, la cui parte reale σ (che si indica con $R(s)$) si suppone per ora >1. Questa funzione numerica $f(n)$ soddisfa mani-

festamente la condizione fondamentale (A); inoltre la serie

$$(6) \qquad \sum |f(n)| = \sum \frac{1}{n^\sigma}$$

è convergente perchè $\sigma > 1$. Supponiamo ora di mantenere $\underline{s}$ in un campo finito (del piano complesso $\underline{s}$, situato tutto a destra della retta $\mathcal{R}(s) = 1$, sia adunque

$$\sigma \geq \sigma_0 > 1 ;$$

in tal caso la serie dei moduli della serie $\sum \frac{1}{n^s}$ sarà, per la (6), minorante rispetto alla serie convergente a termini fissi

$$\sum \frac{1}{n^{\sigma_0}} .$$

Dunque, nel detto campo C, la serie $\sum\limits_n \frac{1}{n^s} = \sum\limits_n e^{-s \log n}$ è convergente assolutamente ed uniformemente; e poichè i termini della serie $e^{-s \log n}$ sono, in C, funzioni finite continue e monodrome della variabile complessa $\underline{s}$, per noti teoremi, anche la somma della serie sarà funzione finita, continua e monodroma in C e, rimanendo in questo campo, potremo applicare, quante volte occorra, la derivazione per serie. Questa funzione di $\underline{s}$, definita per ora nel semipiano $\mathcal{R}(s) > 1$, si indica [illegible] Riemann col simbolo $\zeta(s)$ e si chiama la funzione

zeta-Riemanniana. Essa è dunque (provvisoriamente) definita dalla formola

$$(III) \qquad \zeta(s) = \sum_{n=1}^{n=\infty} \frac{1}{n^s} \quad , \quad \text{per } \mathcal{R}(s) > 1,$$

e in questo campo è una funzione finita continua e monodroma della variabile complessa s. In questo stesso campo $\mathcal{R}(s) > 1$ vale anche, per la (I) d'Eulero, l'altra rappresentazione per prodotto infinito convergente in senso stretto

$$(III^*) \qquad \zeta(s) = \prod_p \frac{p^s}{1-p^s} \qquad (\mathcal{R}(s) > 1),$$

e di qui risulta che: la zeta di Riemann non si annulla mai in questo campo.

Già da questa formola (III*), la $\zeta(s)$ appare essenzialmente legata alla legge di distribuzione dei numeri primi, ed in effetto Riemann, applicando la teoria delle funzioni di variabile complessa, ha dato l'impulso ad una serie di importanti ricerche che pongono in relazione le leggi di frequenza dei numeri primi colla distribuzione dei punti di zero della funzione $\zeta(s)$, estesa secondo le leggi del prolungamento analitico a tutto il piano complesso. Vedremo appunto che: la $\zeta(s)$ è prolungabile analiticamente in tutto il piano

complesso s e rimane ivi funzione finita, continua e monodroma di s, eccetto che nel punto $s=1$ ove ha un polo del 1° ordine col residuo $=1$. (Cfr. più oltre § 60).

Per prepararci la via ad un primo prolungamento analitico della $\zeta(s)$ di Riemann, premettiamo alcune nozioni sulle così dette serie di Dirichlet, sotto il qual nome si comprendono ora tutte le serie della forma

$$(7) \qquad \sum_{n=1}^{n=\infty} a_n e^{-\lambda_n s},$$

dove le a_n sono costanti complesse qualunque e

$$\lambda_1, \lambda_2 \ldots \lambda_n \ldots$$

è una serie illimitatamente crescente di costanti reali colla condizione $\lim_{n=\infty} \lambda_n = \infty$, ed s indica una variabile complessa. Queste serie (7) comprendono le ordinarie serie di potenze quando si faccia $\lambda_n = n$ e si eseguisca il cangiamento di variabile $z = e^{-s}$, in secondo luogo le serie di Dirichlet in senso stretto

$$(8) \qquad \sum \frac{a_n}{n^s}$$

quando si ponga $\lambda_n = \log n$.

A noi basterà trattare di queste ultime, e cominceremo dallo stabilire il lemma:

A) Se una serie (8) di Dirichlet converge per $s = s_0$, in qua-

lunque campo finito del piano s situato tutto a destra della retta $\mathcal{R}(s) = \mathcal{R}(s_0)$ la serie è uniformemente convergente.

Poniamo

$$S_n = \frac{a_1}{1^{s_0}} + \frac{a_2}{2^{s_0}} + \cdots + \frac{a_n}{n^{s_0}} \; ;$$

e, per l'ipotesi della convergenza della serie $\Sigma \frac{a_n}{n^{s_0}}$, queste somme parziali S_n resteranno in modulo limitate uniformemente per tutti i valori di n, cioè essendo A una quantità reale positiva fissa, sarà

$$(9) \qquad |S_n| < A \qquad \text{per qualunque } n.$$

Ora della serie (8) consideriamo la somma $R_{m,p}$ di un numero qualunque p di termini dopo l'm^{ma}

$$(10) \qquad R_{m,p} = \frac{a_{m+1}}{(m+1)^s} + \frac{a_{m+2}}{(m+2)^s} + \cdots + \frac{a_{m+p}}{(m+p)^s} ,$$

e dimostriamo che, preso ε positivo piccolo a piacere, si può prendere m tanto grande che da quell'm in poi, con qualunque p, si abbia

$$|R_{m,p}| < \varepsilon$$

uniformemente pei valori di s nel campo supposto.

Osservando che

$$S_n - S_{n-1} = \frac{a_n}{n^{s_0}} \; ,$$

scriviamo la (10) così:

$$R_{m,p} = \frac{S_{m+1} - S_m}{(m+1)^{s-s_0}} + \frac{S_{m+2} - S_{m+1}}{(m+2)^{s-s_0}} + \cdots + \frac{S_{m+p} - S_{m+p-1}}{(m+p)^{s-s_0}},$$

od anche

$$R_{m,p} = S_{m+1}\left(\frac{1}{(m+1)^{s-s_0}} - \frac{1}{(m+2)^{s-s_0}}\right) + S_{m+2}\left(\frac{1}{(m+2)^{s-s_0}} - \frac{1}{(m+3)^{s-s_0}}\right) + \cdots$$

$$\cdots + S_{m+p-1}\left(\frac{1}{(m+p-1)^{s-s_0}} - \frac{1}{(m+p)^{s-s_0}}\right) + \frac{S_{m+p}}{(m+p)^{s-s_0}} - \frac{1}{(m+1)^{s-s_0}}.$$

Prendendo i moduli e ponendo mente alla (9), avremo (con $s = \sigma + i\tau$, $s_0 = \sigma_0 + i\tau_0$)

$$(11) \quad \left| R_{m+p} \right| < A \sum_{r=1}^{r=p-1} \left| \frac{1}{(m+r)^{s-s_0}} - \frac{1}{(m+r+1)^{s-s_0}} \right| + \frac{A}{(m+p)^{\sigma-\sigma_0}} + \frac{A}{(m+1)^{\sigma-\sigma_0}}.$$

Indicando con x una variabile reale, si ha

$$\frac{d}{dx} x^{-(s-s_0)} = \frac{d}{dx} e^{-(s-s_0)\log x} = -\frac{s-s_0}{x^{s-s_0+1}},$$

e coll'integrazione da $m+r$ a $m+r+1$

$$\frac{1}{(m+r)^{s-s_0}} - \frac{1}{(m+r+1)^{s-s_0}} = (s-s_0)\int_{m+r}^{m+r+1} \frac{dx}{x^{s-s_0+1}}.$$

L'integrale del secondo membro è esteso al tratto dell'asse reale $(m+r,\ m+r+1)$, di ampiezza $=1$, e il modulo dell'integrando $\frac{1}{x^{s-s_0+1}}$ è dato da

$$\frac{1}{x^{\sigma-\sigma_0+1}} \leq \frac{1}{(m+r)^{\sigma-\sigma_0+1}}$$

indi per la formola di Darboux

$$\left| \int_{m+r}^{m+r+1} \frac{dx}{x^{s-s_0+1}} \right| \leq \frac{1}{(m+r)^{\sigma-\sigma_0+1}},$$

e per la (11) possiamo prendere la nuova limitazione

$$\left|R_{m,p}\right| < A\left|s-s_0\right| \sum_{r=1}^{r=p-1} \frac{1}{(m+r)^{\sigma-\sigma_0+1}} + \frac{A}{(m+p)^{\sigma-\sigma_0}} + \frac{A}{(m+1)^{\sigma-\sigma_0}} .$$

Nel campo finito in considerazione, essendo H, k quantità positive fisse, abbiamo $(s-s_0) < H \quad \sigma-\sigma_0 > k > 0$, e la diseguaglianza superiore può a fortiori scriversi

$$\left|R_{m,p}\right| < AH \sum_{r=1}^{r=p-1} \frac{1}{(m+r)^{k+1}} + \frac{A}{(m+p)^{k}} + \frac{A}{(m+1)^{k}} ,$$

Siccome la serie $\sum \frac{1}{n^{k+1}}$ è convergente, possiamo ora prendere $\underline{m}$ tanto grande che si abbia, con qualunque p,

$$\left|R_{m,p}\right| < \varepsilon$$

per tutti i valori di $\underline{s}$ nel nostro campo. Il lemma A) è così stabilito.

§ 46.

Prolungamento analitico della $\zeta(s)$ a tutto il semipiano $\mathcal{R}(s) > 0$. – Residuo nel polo del 1º ordine $s = 1$.

La dimostrazione del lemma A) sulle serie di Dirichlet è tutta fondata sulla diseguaglianza (9), e nell'enunciato del teorema, alla condizione di convergenza per $\sigma = \sigma_0$ si può sostituire l'altra (meno restrittiva) che le somme parziali S_n rimangano limitate in modulo. Segue di qui che per una serie di Dirichlet, che in qualche punto almeno sia convergente, il cam-

po di convergenza sarà un semipiano a destra di una determinata retta $\sigma = \alpha$, parallela all'asse delle quantità immaginarie; questa dicesi la retta di convergenza e il valore α l'ascissa di convergenza. Naturalmente può anche essere $\alpha = -\infty$ e allora la serie converge in tutto il piano (dà una trascendente intera). In ogni caso: in qualunque campo C, tutto interno al campo di convergenza, ha luogo convergenza uniforme, e per ciò la somma della serie

$$f(s) = \sum_1^\infty \frac{a_n}{n^s}$$

è una funzione finita, continua e monodroma della variabile complessa s; la serie può derivarsi termine a termine quante volte si voglia ecc.

Ciò che abbiamo detto fin qui è relativo soltanto alla convergenza uniforme, non alla convergenza assoluta che può anche parzialmente mancare.

Ma si osservi che se per $s = s_0$ la serie di Dirichlet converge, essa converge certo assolutamente per $\mathcal{R}(s) > \mathcal{R}(s_0)+1$, perchè ponendo $s = s_0 + s'$, nella serie dei moduli

$$\sum \frac{|a_n|}{n^\sigma} = \sum \frac{|a_n|}{n^{\sigma_0}} \frac{1}{n^{\sigma'}} \qquad (\sigma' = \mathcal{R}(s'))$$

i termini risultano da quelli della serie convergente

$\sum \frac{1}{n^{\sigma'}}$ $(\sigma' > 1)$ moltiplicandoli per le quantità $\frac{|a_n|}{n^{\sigma_0}}$ che tendono a zero al crescere di $\underline{n}$, essendo convergente $\sum \frac{a_n}{n^{s_0}}$. Così adunque: Se $\sigma = \alpha$ è l'ascissa di convergenza della serie di Dirichlet, almeno al di là della retta $\mathcal{R}(s) = \alpha + 1$ ha luogo anche convergenza assoluta.

Osserviamo inoltre che, se in un punto $s = s_1$ ha luogo convergenza assoluta, a fortiori ciò ha luogo per un punto più a destra, per $\mathcal{R}(s) > \mathcal{R}(s_1)$, perchè

$$\left|\frac{a_n}{n^s}\right| < \left|\frac{a_n}{n^{s_1}}\right|.$$

Ne risulta che, insieme all'ascissa $\sigma = \alpha$ di convergenza semplice avremo una seconda ascissa $\sigma = \beta$ di convergenza assoluta; può anche darsi che sia $\beta = \alpha$ ed allora si avrà sempre convergenza assoluta (al di là di $\sigma = \alpha$); ma in ogni caso sarà $\beta \leq \alpha + 1$. Così nel semipiano di convergenza della serie di Dirichlet abbiamo in generale una prima striscia di ampiezza compresa fra $\underline{0}$ e $\underline{1}$ (limiti inclusi) di convergenza condizionata, seguita da tutto un semipiano di convergenza assoluta.

Un esempio notevole ed importante per il prolungamento analitico della $\zeta(s)$, è quello dato dalla serie

di Dirichlet

$$(12) \qquad 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots$$

Qui per s reale > 0 la serie converge; invece per $s = 0$ non converge, onde risulta dai teoremi superiori che: il suo campo di convergenza è il semipiano a destra dell'asse immaginario $\mathcal{R}(s) > 0$. E siccome per $s = 1$ la serie converge bensì, ma condizionatamente, vediamo che nel caso attuale la striscia di convergenza condizionata ha l'ampiezza massima $0 \leq \mathcal{R}(s) \leq 1$. Al di là di $\mathcal{R}(s) = 1$ abbiamo convergenza assoluta.

Posto ora

$$f(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \cdots = \sum_1^\infty \frac{(-1)^{n-1}}{n^s},$$

la $f(s)$ sarà in tutto il semipiano $\mathcal{R}(s) > 0$ funzione finita, continua e monodroma di s. D'altra parte nel semipiano $\mathcal{R}(s) > 1$, dove abbiamo sopra definito la $\zeta(s)$ Riemanniana la $f(s)$ è legata a questa da una semplicissima relazione che troviamo costruendo $(1 - 2^{1-s})\zeta(s)$. A causa della convergenza assoluta di

$$\zeta(s) = \sum \frac{1}{n^s} \qquad \text{per } \mathcal{R}(s) > 1,$$

abbiamo infatti

$$(1 - 2^{1-s})\zeta(s) = \sum_1^\infty \frac{1}{n^s} - 2\sum_1^\infty \frac{1}{(2n)^s},$$

cioè

$$(1-2^{1-s})\zeta(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots .$$

Abbiamo così trovata la relazione

$$(IV) \qquad (1-2^{1-s})\zeta(s) = f(s) \qquad \left(f(s) = \sum_1 \frac{(-1)^{n-1}}{n^s}\right),$$

la quale è valida dapprima nel semipiano $\mathcal{R}(s) > 1$. Ma, siccome $f(s)$ esiste ed è regolare in tutto il semipiano $\mathcal{R}(s) > 0$, questa formola ci dà appunto il prolungamento analitico della funzione di Riemann $\zeta(s)$ a tutto il semipiano $\mathcal{R}(s) > 0$, l'asse delle quantità immaginarie escluso. Ora si osservi che la funzione

$$1 - 2^{1-s} = 1 - e^{(1-s)\log 2}$$

è una trascendente intera, che si annulla del 1° ordine nei punti

$$(13) \qquad s = 1 + \frac{2k\pi i}{\log 2} \qquad (k \text{ intero}),$$

situati sulla retta limite $\mathcal{R}(s) = 1$ del semipiano, nel quale la $\zeta(s)$ era prima definita. Dunque, tutto al più, la funzione

$$\zeta(s) = \frac{f(s)}{1-2^{1-s}},$$

(la $f(s)$ essendo regolare sulla $\mathcal{R}(s) = 1$) potrà avere, in uno o più dei punti (13) dei poli del 1° ordine, se ivi la $f(s)$ non si annulla. Intanto per uno dei punti (13), e

cioè pel punto $s=1$ (corrispondente a $k=0$) questo accade certamente, perchè

$$f(1) = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots = \log 2$$

non è nulla. Dunque in $s=1$ la $\zeta(s)$ Riemanniana ha un polo del 1° ordine, e noi ne calcoliamo subito il residuo da quello di $\frac{1}{1-2^{1-s}}$, che è

$$\lim_{s=1} \frac{s-1}{1-2^{1-s}} = \frac{1}{\log 2} \quad \text{(p.e. dalla regola de l'Hopital)},$$

e il residuo della $\zeta(s)$ è dunque $=1$. Quanto agli altri punti (13), per $k \neq 0$, si dimostrerà in seguito (al § 60) che essi sono regolari per $\zeta(s)$, che cioè sono altrettanti zeri per la $f(s)$. E intanto concludiamo:

La funzione $\zeta(s)$ di Riemann esiste certamente, come funzione meromorfa di $\underline{s}$, in tutto il semipiano $R(s)>0$ e nel punto $s=1$ ha un polo del 1° ordine col residuo $=1$, corrispondente alla formula

$$\text{(V)} \qquad \lim_{s=1} \left\{ (s-1)\zeta(s) \right\} = 1.$$

E qui arrestiamo per ora lo studio di queste prime proprietà della $\zeta(s)$ di Riemann, che si ritrovano generalizzate per una funzione analoga in ogni corpo K algebrico, la funzione Zèta di Dedekind, di cui vogliamo subito occuparci.

§ 47.

La funzione $\zeta_K(s)$ di Dedekind definita nel semipiano $R(s)>1$ Sue prime proprietà.

Seguendo la via tracciata da Dirichlet, che determinò per via trascendente il numero delle classi delle forme binarie quadratiche, Dedekind ha dato una formola per risolvere il problema più generale della determinazione del numero h delle classi di ideali in un corpo algebrico qualunque K. Questa formola si fonda essenzialmente sulla introduzione di una funzione $\zeta_K(s)$, inerente al corpo K, e che generalizza, ad un corpo algebrico K di grado n qualunque, la funzione $\zeta(s)$ di Riemann, alla quale la $\zeta_K(s)$ si riduce quando $n=1$, cioè quando K diventa il corpo dei numeri razionali.

La funzione $\zeta_K(s)$ di Dedekind si definirà, dapprima nel semipiano $R(s)>1$, in modo analogo come la $\zeta(s)$ Riemanniana dalla formula (III) § 45.

Nel corpo algebrico dato K, di grado n, indichiamo con A un ideale variabile, che percorra la serie infinita di tutti gli ideali, e con P un ideale primo, che percorra la serie (pure infinita) di tutti gli ideali pri=

ni. Cominciamo dal dimostrare:

a) <u>Se la variabile complessa s ha la parte immaginaria $\sigma = \mathcal{R}(s) > 1$, il prodotto infinito</u>

$$(1) \qquad \prod_P \frac{1}{1 - \frac{1}{(NP)^s}}$$

<u>esteso a tutti gli ideali primi P del corpo K, è convergente assolutamente in senso stretto.</u> – Secondo le proprietà $b)$ $c)$, ricordate al § 44, basterà dimostrare che è convergente la serie (a termini positivi)

$$(2) \qquad \sum_P \frac{1}{(NP)^\sigma} \qquad \text{per } \sigma > 1.$$

Sia p il numero primo ordinario coordinato all'ideale primo P, onde sarà $NP = p^f$ con $1 \leq f \leq n$. Il numero primo p si decompone, al massimo, in n ideali primi diversi e se supponiamo

$$p = P_1 P_2 \cdots P_q,$$

dove i q ideali primi a destra sono diversi od anche eguali, è $q \leq n$, e la somma dei termini nessa serie (1), appartenenti a questo numero primo p, è data da

$$\frac{1}{p^{f_1\sigma}} + \frac{1}{p^{f_2\sigma}} + \cdots + \frac{1}{p^{f_q\sigma}};$$

e siccome ciascun f è ≥ 1, questa è minorante rispetto a $\frac{q}{p^\sigma}$, e in ogni caso $\leq \frac{n}{p^\sigma}$.

La serie (1) è dunque minorante rispetto alla serie

$$n \sum \frac{1}{p^{\sigma}} ,$$

che converge, essendo $\sigma > 1$.

Passiamo ora a considerare la serie

$$(3) \qquad \sum_{A} \frac{1}{(NA)^s} ,$$

dove A percorre tutti gli ideali del corpo K, e dimostriamo che, in ogni campo finito tutto interno al semipiano $\mathcal{R}(s) > 1$, questa serie converge assolutamente ed uniformemente e rappresenta quindi una funzione della variabile complessa s regolare in tutto l'interno del semipiano; questa sarà la funzione $\zeta_K(s)$ di Dedekind, di cui studieremo poi il prolungamento a tutto il piano.

Intanto, trattandosi di stabilire la convergenza assoluta, per ciò incondizionata, della serie (3) (per $\mathcal{R}(s) > 1$), noi cominceremo dall'osservare che ciascun termine

$$\frac{1}{m^s}$$

della serie (3) si troverà ripetuto tante volte quanti sono gli ideali A del corpo che hanno la stessa norma $NA = m$. Sappiamo dal § 29 che questo numero di ideali, per ogni dato m razionale intero positivo, è sempre finito, e indicandolo con $F(m)$, raggruppando i termini egua-

li, potremo scrivere la (3) sotto la forma

$$(4) \qquad \sum \frac{1}{(NA)^s} = \sum_m \frac{F(m)}{m^s},$$

dove a destra, ordinando per valori crescenti di $\underline{m}$, abbiamo una serie di Dirichlet (§ 45).

Se poniamo $s = \sigma + i\tau$, la serie dei moduli della (3) è

$$(5) \qquad \sum \frac{1}{(NA)^\sigma},$$

e noi andiamo a dimostrare che questa è convergente. Ne risulterà la convergenza assoluta della (3), cioè per la (4) della serie di Dirichlet equivalente

$$\sum_m \frac{F(m)}{m^s},$$

dopo di che, dai teoremi ai §§ 45 e 46, sulle serie di Dirichlet, risulterà che in tutto l'interno del semipiano $R(s) > 1$ la serie (3) è anche uniformemente convergente.

Per provare la convergenza della serie (5), prendiamo il prodotto infinito assolutamente convergente in senso proprio (per quando precede):

$$(6) \qquad \prod_P \frac{1}{1 - \frac{1}{(NP)^\sigma}} = Q$$

e disponiamo dell'ordine (arbitrario) dei fattori ordinandoli per norma NP crescente, talchè verranno raggruppati tutti quelli che presentano la stessa norma.

Sia ora m un intero razionale positivo, che faremo poi crescere infinitamente, e del prodotto infinito (6) consideriamo quel prodotto parziale finito in cui $NP \leq m$, indichiamolo con

$$\prod_{NP \leq m} \left(\frac{1}{1-\frac{1}{(NP)^\sigma}} \right).$$

Qui, come al § 44, sviluppiamo ciascuno dei fattori nella progressione geometrica

$$\frac{1}{1-\frac{1}{(NP)^\sigma}} = 1 + \frac{1}{(NP)^\sigma} + \frac{1}{(NP)^{2\sigma}} + \frac{1}{(NP)^{3\sigma}} + \cdots,$$

e moltiplichiamo questo numero finito di serie fra loro (cfr. § 44). Otterremo così una parte della serie (5), che indicheremo con $\sum' \frac{1}{(NA)^\sigma}$, dove figureranno tutti e soli gli infiniti ideali A che non sono divisibili per alcun ideale primo di $NP > m$. Fra questi figurano certamente tutti gli ideali A di norma $NA \leq m$, e poi altri (infiniti) ideali di $NA > m$, e possiamo quindi decomporre $\sum' \frac{1}{(NA)^\sigma}$ nelle due parti $\sum_{NA \leq m} \frac{1}{(NA)^\sigma} + \sum'_{NA > m} \frac{1}{(NA)^\sigma}$, di cui la prima è un polinomio, la seconda una serie.

Così abbiamo

$$(7) \qquad \prod_{NP \leq m} \frac{1}{1-\frac{1}{(NP)^\sigma}} = \sum_{NA \leq m} \frac{1}{(NA)^\sigma} + \sum_{NA > m} \frac{1}{(NA)^\sigma},$$

e ne risulta intanto che $\sum_{NA\leq m}\frac{1}{(NA)^\sigma}$ è inferiore al valore del prodotto (finito) a sinistra, e a fortiori quindi a quello del prodotto infinito (6), giacchè i fattori di questo sono tutti >1; dunque si ha

$$\sum_{NA\leq m}\frac{1}{(NA)^\sigma} < \prod_P \frac{1}{1-\frac{1}{(NP)^\sigma}} < Q\,.$$

Questa limitazione vale per quanto grande si prenda il numero m, e ne risulta manifestamente che nella serie a termini positivi (5) tutte le somme parziali sono limitate $< Q$, e per ciò la serie stessa è convergente c. d. d. Di più dalla eguaglianza (7), passando al limite per $m=\infty$, siccome la seconda somma $\sum'$ tende manifestamente a zero, ne risulta l'identità fra il valore della serie (5) e del prodotto infinito (6). Ma ora osserviamo di più che la formola (7), pel modo stesso come è stata dedotta, sta anche se per l'esponente σ poniamo invece s complesso qualunque purchè $\mathcal{R}(s)>1$:

$$\prod_{NP\leq m}\frac{1}{1-\frac{1}{(NP)^s}} = \sum_{NA\leq m}\frac{1}{(NA)^s} + \sum_{NA>m}{}'\frac{1}{(NA)^s}$$

e di qui, passando al limite per $m=\infty$, a causa della

convergenza dimostrata dal prodotto infinito (1) e della serie (3), deduciamo la loro identità:

$$\sum_A \frac{1}{(NA)^s} = \prod_P \frac{1}{1-\frac{1}{(NP)^s}} \qquad (\text{per } \mathcal{R}(s)>1).$$

Siamo così giunti al risultato finale:

La formola

$$(I) \qquad \zeta_K(s) = \sum_A \frac{1}{(NA)^s} \qquad (\mathcal{R}(s)>1)$$

in tutto il semipiano $\mathcal{R}(s)>1$ definisce la $\zeta_K(s)$ di Dedekind come funzione finita, continua e monodroma della variabile complessa s, convergendo la serie a destra uniformemente in ogni regione interna al detto semipiano.

Della funzione stessa si può dare il secondo sviluppo per prodotto infinito, convergente in senso stretto nella medesima regione,

$$(II) \qquad \zeta_K(s) = \prod_P \frac{1}{1-\frac{1}{(NP)^s}} \qquad (\mathcal{R}(s)>1).$$

Questa seconda rappresentazione analitica pone in evidenza che: almeno nell'interno del semipiano $\mathcal{R}(s)>1$, la $\zeta_K(s)$ non si annulla mai.

Naturalmente se si suppone che il corpo algebrico K si riduca al corpo razionale $(n=1)$, le formole precedenti (I), (II) si riducono a quelle di partenza (III), (III*) per

la definizione, nel semipiano $\Re(s)>1$, della $\zeta(s)$ Riemanniana, alla quale si riduce allora la $\zeta_K(s)$ di Dedekind.

Ma, ritornando al caso generale di un corpo algebrico K di grado n, noi possiamo decomporre la $\zeta_K(s)$ di Dedekind in tante funzioni zeta parziali quante unità sono nel numero h delle classi, prendendo nella serie a destra in (I) soltanto quei termini che corrispondono ad ideali A appartenenti a una medesima classe. Se diciamo H la classe, scriveremo la relativa somma parziale così

$$\sum_{A \text{ in } H} \frac{1}{(NA)^s},$$

e questa, come parte della serie totale $\sum \frac{1}{(NA)^s}$, assolutamente e uniformemente convergente, avrà pure una convergenza della stessa specie, nell'interno del semipiano $\Re(s)>1$; la sua somma sarà dunque una funzione finita, continua e monodroma di s nella detta regione. Indicando questa zeta parziale con $\zeta_K(s;H)$, avremo dunque

$$\text{(III)} \qquad \zeta_K(s;H)=\sum_{A \text{ in } H} \frac{1}{(NA)^s}, \qquad (\Re(s)>1)$$

e sarà manifestamente

$$\zeta_K(s)=\sum_H \zeta_K(s;H),$$

la somma a destra constando di h termini corrispondenti alle h classi. Si osservi che se dalla classe H si estrae un ideale A_1, gli ideali A in H sono tutti e soli gli equivalenti ad A_1 e, in luogo della notazione (III), possiamo allora anche usare l'altra

$$\text{(III*)} \qquad \zeta_K(s;\, A_1) = \sum_{A \sim A_1} \frac{1}{(NA)^s}, \qquad (\Re(s) > 1).$$

In particolare gli ideali della classe principale sono quelli principali (α) generati da tutti i numeri interi del corpo, nella qual cosa però è da tener presente che gli infiniti numeri associati ad α dànno tutti un medesimo ideale. Così la zèta parziale corrispondente alla classe principale potrà scriversi

$$\zeta_K(s;1) = \sum_{\alpha} \frac{1}{(N\alpha)^s},$$

dove a destra il numero α percorre gli interi del corpo, così però che di ciascuna serie di numeri associati si prenda un solo numero α. Più in generale per ciascuna zèta parziale sussiste una formola analoga alla superiore, che si ottiene nel modo seguente.

Dalla classe inversa H^{-1} di H si estragga un ideale fisso B (un moltiplicatore), talchè $AB = (\xi)$ sarà un ideale principale, e il numero ξ sarà nell'ideale B, cioè divi-

sibile per B. Viceversa un numero ξ di B dà un ideale principale (ξ) divisibile per B, e, ponendo $(\xi) = AB$, l'ideale A appartiene ad H; d'altra parte $N(\xi) = |N\xi| = NA \cdot NB$, che scriviamo $\frac{1}{(NA)^s} = \frac{(NB)^s}{|N\xi|^s}$, e la formula (III) diventa

$$(\text{IV}) \qquad \zeta_K(s,H) = (NB)^s \sum_\xi \frac{1}{|N\xi|^s},$$

dove a destra B indica un ideale fisso della classe inversa H^{-1} e il numero ξ percorre tutti i numeri dall'ideale B, però uno solo di ciascuna serie di numeri associati. [Risulta di qui implicitamente che l'espressione a destra in (IV) non varia cangiando B in un ideale equivalente, ciò che è anche manifesto perchè NB e $|N\xi|$ acquistano un medesimo fattore].

Ed ora per la funzione $\zeta_K(s)$ di Dedekind, e per le zeta parziali $\zeta_K(s,H)$ si presentano le medesime questioni sul prolungamento analitico, di cui abbiamo iniziato lo studio al § 46 per la $\zeta(s)$ Riemanniana. Tali questioni vennero risolute nel modo più completo dalle notevolissime ricerche di Hecke, delle quali diremo più oltre. Qui, pel problema della determinazione del numero h delle classi di ideali, occorre soltanto esaminare il comportamento della $\zeta_K(s)$ quan-

do s, per valori reali >1, si accosta al valore critico $s=1$ e dimostrare che

$$(s-1)\,\zeta_K(s)$$

tende verso un limite determinato e finito non nullo, che sta appunto in una relazione semplicissima col numero h delle classi.

§ 48.

Preliminari alla determinazione del numero h delle classi. - Numeri ridotti rispetto ad un sistema fondamentale di unità.

Alle ricerche per la determinazione dell'anzidetto limite dobbiamo premettere la dichiarazione che: le nozioni di equivalenza di ideali, numero delle classi, ideali principali ecc. s'intenderanno qui nel senso ristretto a cui già abbiamo accennato al § 38, e cioè: due ideali A, $\bar{A}$ si diranno equivalenti solo quando i numeri dell'uno siano proporzionali ai numeri dell'altro per un numero frazionario σ di norma positiva. Un ideale si dirà principale $A=(\alpha)$ solo quando venga generato da un numero α di norma positiva, e corrispondentemen-

te per unità ε intenderemo esclusivamente unità di norma $N\varepsilon = +1$. I teoremi sulle classi, sulla loro composizione ecc. rimangono validi in questa definizione più ristretta dell'equivalenza, e così pure i teoremi di Dirichlet sulle unità (§§ 20-22) ristretti alla considerazione delle unità di norma $= +1$ (cfr. particolarmente § 22).

Ciò premesso, ecco quale è la ricerca fondamentale a cui dobbiamo ora rivolgerci.

Sia A un qualunque ideale, e prendiamo in considerazione i numeri α di A di norma $N\alpha$ positiva, i quali generano gli ideali principali (nel senso ristretto) che sono divisibili per A. Se con t indichiamo una variabile positiva che facciamo poi crescere all'infinito, per ogni valore assegnato a t il numero di questi ideali principali diversi divisibili per A, la cui norma non supera t, è in ogni caso un numero finito T (perchè gli ideali di egual norma sono sempre in numero finito (§ 29 c)). Così, per ogni valore dato alla variabile positiva t, la T ha un valore positivo o nullo), che va manifestamente cre

scendo all'infinito quando t cresce infinitamente.
Ora quello che importa per noi dimostrare è che:

A) <u>Il rapporto $\frac{T}{t}$, al crescere infinito di t, converge verso un limite determinato e finito, che ha la forma</u>

$$(I) \qquad \lim_{t=\infty}\left(\frac{T}{t}\right)=\frac{g}{NA},$$

<u>dove g è una costante positiva indipendente dall'ideale A.</u>

[Nel caso ovvio del corpo K razionale, $n=1$, ogni ideale è un ideale principale (a), generato da un numero intero positivo $\underline{a}$, ed è immediato che si ha $T=E\left(\frac{t}{a}\right)$, il simbolo $E(x)$ indicando il massimo intero contenuto in $x>0$. Qui si ha $T\leq\frac{t}{a}<T+1$ e perciò $\frac{1}{a}-\frac{1}{t}<\frac{T}{t}\leq\frac{1}{a}$, indi $\lim_{t=\infty}\left(\frac{T}{t}\right)=\frac{1}{a}$, che rientra nella formola (I) con $g=1$].

Per dimostrare la formola (I) conviene in primo luogo osservare che gli ideali principali (α) divisibili per A si generano dai numeri α <u>di norma positiva</u> contenuti in A. Però ciascuno di questi ideali, ove $\underline{\alpha}$ percorra tutti gli interi di A (di norma positiva), viene generato anche da tutti e soli i numeri associati ad α, cioè della forma $\varepsilon\alpha$ ove ε indica un'unità di norma $=+1$. Perciò, salvo nel caso dei corpi quadra-

tratici immaginarî, essendo infinito il numero di queste unità, ciascuno di questi ideali viene così ripetuto infinite volte, e la prima cosa che occorre fare è di scegliere nella serie infinita degli associati uno di questi numeri, ovvero un numero finito di essi, in guisa che ciascuno degli ideali divisibili per A venga così generato o una sola volta o un numero fisso di volte. Questo si ottiene assoggettando il numero α, ed i suoi coniugati, a soddisfare, coi loro moduli, a certe limitazioni, che verranno verificate solo da un numero finito di essi nella serie associata, e che si diranno per ciò numeri <u>ridotti</u>. A fondamento di questa ricerca stanno i risultati di Dirichlet sulla distribuzione delle unità, che abbiamo stabilito nei §§ 20-22, applicati però in senso ristretto (cfr. § 22) cioè nel caso in cui le unità di cui si tratta siano tutte di norma $= +1$. Riprendiamo per ciò le notazioni dei paragrafi citati e supponiamo che degli n corpi coniugati ve ne siano <u>r</u> reali e <u>s</u> coppie di complessi coniugati immaginarii, dove $n = r + 2s$. Ponendo ancora $\nu = r + s$, sappiamo che esistono nel corpo $\nu-1$

unità fondamentali dai prodotti delle cui potenze, combinate con un numero finito di unità ridotte, nascono tutte le unità del corpo. Per abbreviare la ricerca, riferiamoci senz'altro ad un sistema <u>fondamentale</u> $(\varepsilon_1, \varepsilon_2 \cdots \varepsilon_{\nu-1})$ di unità, nel qual caso le k unità ridotte $\rho_1, \rho_2 \cdots \rho_k$ sono le radici m^{me} dell'unità contenute in $K(\theta)$ e tutte le unità ε vengono date, una ed una sola volta, dalla formola (§ 22)

$$(1) \qquad \varepsilon = \rho\varepsilon_1^{m_1}\,\rho\varepsilon_2^{m_2}\cdots\rho\varepsilon_{\nu-1}^{m_{\nu-1}} \begin{cases} \rho = \rho_1, \rho_2 \cdots \rho_k \\ m_i = 0, 1, 2, 3 \ldots \end{cases}$$

Ed ora, come al § 20 abbiamo definiti i logaritmi coniugati delle unità, così ora definiamo più in generale i logaritmi coniugati di un qualunque numero α intero in $K(\theta)$. Riprendiamo per ciò i ν corpi coniugati

$$K^{(1)}, K^{(2)} \cdots K^{(\nu)},$$

del § 20, dei quali i primi r reali, i seguenti $\nu - r$ complessi, che insieme ai precedenti ed ai loro complessi coniugati, dànno tutti gli n corpi coniugati. Essendo α un intero qualunque in $K(\theta)$ di norma $N\alpha$ positiva, indicheremo con $l_q(\alpha)$ $(q = 1, 2, \cdots \nu)$, e chiameremo

logaritmo q^{mo} coniugato del numero α, la parte reale di

$$\log \alpha^{(q)} - \frac{1}{n} \log N\alpha \,, \quad \text{se } K^{(q)} \text{ è un corpo reale.}$$

e invece il doppio della stessa parte reale, se $K^{(q)}$ è immaginario. Ponendo ciascun numero $\alpha^{(q)}$ sotto la forma trigonometrica

$$\alpha^{(q)} = R_q \, e^{2 i \omega_q} \,,$$

abbiamo dunque

$$(2) \quad \begin{cases} l_q(\alpha) = \log R_q - \frac{1}{n} \log N\alpha \,, & \text{se } q = 1, 2, \dots r \\ l_q(\alpha) = 2 \log R_q - \frac{2}{n} \log N\alpha \,, & \text{se } q = r+1 \dots \nu \end{cases}$$

Ne segue

$$l_1(\alpha) + l_2(\alpha) + \dots + l_\nu(\alpha) = \log(R_1 R_2 \cdots R_r R_{r+1}^2 \cdots R_\nu^2) - \log N\alpha,$$

e siccome il numero $N\alpha$ (positivo) ha appunto per modulo $R_1 R_2 \cdots R_{r+1}^2 \cdots R_\nu^2$, vediamo che sussiste in generale l'identità (cfr. § 20)

$$(3) \qquad l_1(\alpha) + l_2(\alpha) + \dots + l_\nu(\alpha) = 0 \,.$$

Inoltre è chiaro, dalle (2), che per due interi qualunque α, β si ha sempre

$$(4) \qquad l_q(\alpha\beta) = l_q(\alpha) + l_q(\beta) \,.$$

Dopo ciò, come al § 21 abbiamo definito gli esponenti $e_1 \; e_2 \dots e_{\nu-1}$ di una qualunque unità rispetto al sistema fondamentale di unità $(\varepsilon_1 \,, \varepsilon_2 \cdots \varepsilon_{\nu-1})$, così

ora possiamo estendere questa nozione ad un qualunque numero $\underline{\alpha}$. Prendiamo infatti il sistema delle $\underline{v}$ equazioni lineari con $v-1$ incognite $e_1, e_2 \dots$ $\dots e_{v-1}$ (cfr. § 21 (3)).

$$\begin{cases} l_{11} e_1 + l_{12} e_2 + \dots + l_{1,v-1} e_{v-1} = l_1(\alpha) \\ l_{21} e_1 + l_{22} e_2 + \dots + l_{2,v-1} e_{v-1} = l_2(\alpha) \\ \dots \dots \dots \dots \dots \dots \\ l_{v1} e_1 + l_{v2} e_2 + \dots + l_{v,v-1} e_{v-1} = l_v(\alpha), \end{cases}$$

le quali sommate dànno l'identità a causa della (3), e delle particolari $\sum_{q=1}^{q=v} l_{qi} = 0 \quad (i = 1, 2, \dots v-1)$, mentre le prime $\underline{v-1}$ di esse, essendo il determinante

$$\mathcal{L}(\varepsilon_1, \varepsilon_2 \dots \varepsilon_{v-1}) = \begin{vmatrix} l_{11} & l_{12} & \dots & l_{1,v-1} \\ \dots & \dots & \dots & \dots \\ l_{v-1,1} & l_{v-1,2} & \dots & l_{v-1,v-1} \end{vmatrix} \neq 0$$

forniranno, risolute, i valori (reali) cercati degli esponenti $e_1, e_2 \dots e_{v-1}$ del numero α.

Se al numero α si sostituisce un numero associato, moltiplicando $\underline{\alpha}$ per un'unità ε data dalla formola (1), a causa della (4) [essendo nulli gli esponenti di un'unità ρ ridotta, $(m_1, 0 \dots 0)$ quelli di ε, ecc.] ciascun esponente e_i di α viene accresciuto di m_i e

si può quindi, in uno ed in un sol modo disporre dei numeri interi $m_1, m_2 \cdots m_{\nu-1}$ in guisa che, per gli esponenti di $\varepsilon\alpha_1$, valgano le limitazioni

$$(5) \qquad 0 \leq e_i < 1 \qquad (i = 1, 2, \cdots \nu-1).$$

Ma in ciò l'unità ridotta moltiplicatrice ρ si può ancora scegliere ad arbitrio fra le $\underline{k}$: $\rho_1, \rho_2 \cdots \rho_k$. Se chiamiamo dunque ridotto un numero α, rispetto al sistema fondamentale di unità $(\varepsilon_1, \varepsilon_2, \cdots \varepsilon_{\nu-1})$, quando i suoi esponenti soddisfano alle condizioni (5) (sono tutti < 1 e non negativi), vediamo che:

In ogni serie di numeri associati ad un numero α (di norma positiva) vi sono sempre k e k soltanto numeri ridotti diversi (quante sono le unità ridotte). Ne consegue che: se facciamo percorrere ad α tutti i numeri ridotti dell'ideale A, ogni ideale principale (α), divisibile per A, viene ripetuto precisamente k volte.

Certanto, avendo sopra indicato con T il numero degli ideali principali divisibile per A, la cui norma non supera t, ne deduciamo:

Il numero dei numeri ridotti α, contenuti nel-

l'ideale A, e la cui norma soddisfa le diseguaglianze

(6) $$0 < N\alpha \leq t,$$

è dato precisamente da kT.

§ 49

Introduzione di variabili continue. Calcolo del limite di $\frac{T}{t}$ ridotto alla valutazione di un integrale multiplo

Riferiamo l'ideale dato A ad una determinata base, sia $[\alpha_1, \alpha_2 \cdots \alpha_n]$, talchè ogni numero α dell'ideale sarà dato da

(7) $$\alpha = h_1\alpha_1 + h_2\alpha_2 + \cdots + h_n\alpha_n,$$

ove le h_i ricevono valori razionali interi. Le condizioni (6) di riduzione imporranno agli interi h_i delle limitazioni, che saranno soddisfatte solo da un numero finito di sistemi delle h_i, precisamente da kT. Come al § 37, coordiniamo alla base dell'ideale A e de' suoi coniugati, le n forme lineari in n variabili indipendenti reali $x_1, x_2 \cdots x_n$

(7*) $$\varphi^{(i)} = \alpha_1^{(i)}x_1 + \alpha_2^{(i)}x_2 + \cdots + \alpha_n^{(i)}x_n$$

il cui determinante è $= NA.\sqrt{D}$ (§ 24), e poniamo

$$\mathfrak{N} = \varphi^{(1)}\varphi^{(2)} \cdots \varphi^{(n)},$$

talchè $\frac{\mathfrak{U}}{N(A)}$ sarà la forma decomponibile del § 37 coordinata all'ideale A.

Quando alle $\underline{x}_i$ attribuiamo valori interi h_i, le $\varphi^{(1)}, \varphi^{(2)} \cdots \varphi^{(n)}$ diventano $\alpha^{(1)}, \alpha^{(2)} \dots \alpha^{(n)}$ ed $\mathfrak{U}$ diventa $N\alpha$. Estendiamo allora alle variabili continue x le nozioni di logaritmi coniugati $l_i(\alpha)$ e di esponenti $e_1(\alpha)$, $e_2(\alpha) \cdots e_{\nu-1}(\alpha)$, introducendo nuove ν variabili reali $y_1, y_2, \cdots y_\nu$, definite da ciò che y_i $(i = 1, 2, \cdots \nu)$ indichi la parte reale di

$$(8) \qquad \log \varphi^{(i)} - \frac{1}{n} \log \mathfrak{U} \text{ , se } K^{(i)} \text{ è un corpo reale,}$$

ed invece il suo doppio se $K^{(i)}$ è immaginario, e le variabili $y_1, y_2, \cdots y_\nu$ saranno così legate dalla relazione

$$(9) \qquad y_1 + y_2 + \cdots + y_\nu = 0.$$

Ed ora al posto degli esponenti $e_1, e_2 \cdots e_{\nu-1}$ introduciamo le $\underline{\nu-1}$ variabili reali $z_1, z_2, \dots z_{\nu-1}$ individuate in funzione (lineare) delle y dalle ν relazioni (dipendenti e compatibili

$$(10) \qquad \begin{cases} l_{11} z_1 + l_{12} z_2 + \cdots + l_{1,\nu-1} z_{\nu-1} = y_1 \\ l_{21} z_1 + l_{22} z_2 + \cdots + l_{2,\nu-1} z_{\nu-1} = y_2 \\ \cdots\cdots\cdots\cdots\cdots \\ l_{\nu 1} z_1 + l_{\nu 2} z_2 + \cdots + l_{\nu,\nu-1} z_{\nu-1} = y_\nu \end{cases}$$

Ad ogni sistema di valori delle $\underline{x}$ pel quale la forma U non si annulli corrisponderà così un sistema perfettamente determinato e finito di valori per $z_1, z_2, \dots z_{\nu-1}$

Dopo ciò, corrispondentemente alle diseguaglianze (5), (6), restringiamo la variabilità delle $x_1, x_2 \dots x_n$ in guisa da soddisfare le diseguaglianze

$$(11) \qquad 0 \leq z_i < 1 \qquad (i = 1, 2, \dots \nu-1)$$

$$(12) \qquad 0 < U \leq 1.$$

Così definiremo un certo campo C, nello spazio a $\underline{n}$ dimensioni delle variabili $x_1, x_2 \dots x_n$, nell'interno del quale $x_1, x_2 \dots x_n$ restano limitate. Poichè in virtù delle (10) e delle (11) restano così limitate $y_1, y_2 \dots y_\nu$, e pel significato (8) di queste y_i e per la (12) restano limitati i moduli di $\varphi^{(1)}, \varphi^{(2)}, \dots \varphi^{(\nu)}$, cioè anche i moduli di $\varphi^{(1)}, \varphi^{(2)} \dots \varphi^{(n)}$. E allora se dalle n equazioni lineari (7*), con determinante $NA\sqrt{D}$ diverso da zero, si traggono le $x_1, x_2, \dots x_n$, queste pure risultano manifestamente limitate.

Ora, essendo $\underline{t}$ un valore positivo fisso comunque grande, pongasi

(13) $$\delta = \frac{1}{\sqrt[n]{t}},$$

e facciasi

(14) $$x_1 = \delta h_1, \quad x_2 = \delta h_2, \ldots x_n = \delta h_n,$$

colle h_i interi razionali. Le $\varphi^{(1)}, \varphi^{(2)}, \ldots \varphi^{(n)}$ diventano allora

$$\delta\alpha^{(1)}, \delta\alpha^{(2)} \ldots \delta\alpha^{(n)} \quad (\alpha^{(i)} = h_1\alpha_1^{(i)} + h_2\alpha_2^{(i)} + \cdots + h_n\alpha_n^{(i)}),$$

cioè i multipli, secondo δ, dei coniugati dell'intero $\alpha = h_1\alpha_1 + \cdots + h_n\alpha_n$, la U viene a coincidere con $\delta^n N\alpha = \frac{N\alpha}{t}$, le $y_1, y_2 \ldots y_\nu$ con $l_1(\alpha), l_2(\alpha) \ldots l_\nu(\alpha)$ rispettivamente, indi $z_1, z_2, \ldots z_{\nu-1}$ con $e_1, e_2, \ldots e_{\nu-1}$. Per ciò valendo le diseguaglianze (11), (12), ne seguono ora, per gli speciali valori (14) delle x, le (5) e (6); ma anche inversamente dalle (5), (6), per valori delle x della forma (14), seguono le (11), (12).

In ordine a quanto si è visto al paragrafo precedente, ne risulta dunque:

<u>Il numero dei punti interni al campo C dello spazio $(x_1, x_2, \ldots x_n)$ a n dimensioni, definite dalle diseguaglianze (11), (12), con coordinate $x_1, x_2 \ldots x_n$ della forma (14) è dato precisamente da kT.</u>

Ora nello spazio $R_n \equiv (x_1, x_2, \ldots x_n)$ consideriamo tut-

ti di coordinate

$$(15) \qquad (\delta h_1, \delta h_2, \cdots \delta h_n) \qquad h_i = 0, \pm 1, \pm 2, \cdots$$

e, attorno a ciascuno di essi come centro, descriviamo il solido parallelepipedo racchiuso dai $2n$ iperpiani

$$x_i = \delta h_i \pm \frac{\delta}{2} \qquad (i = 1, 2, \cdots n);$$

lo spazio R_n resta completamente riempito da questo reticolato di parallelepipedi a ciascuno dei quali compete il volume δ^n (valore dell'integrale n^{plo} $\int_{(n)} \cdots \int dx_1 \cdots dx_n$ esteso a uno dei detti parallelepipedi). Ma allora consideriamo soltanto quei parallelepipedi, i cui centri cadono nei punti (15) interni al nostro campo C, e che appartengono quindi totalmente o parzialmente a C stesso. Il loro numero è kT, e se noi introduciamo il volume V del campo C come dato dall'integrale n^{plo}

$$(16) \qquad V = \iint_{(n)} \cdots \int dx_1\, dx_2 \cdots dx_n\,,$$

esteso al campo C, per la definizione stessa d'integrale n^{plo}, sarà

$$V = \lim_{\delta = 0} (\delta^n kT) = \lim_{t = \infty} \frac{kT}{t},$$

cioè

$$(17) \qquad \lim_{t=\infty} \left(\frac{T}{t}\right) = \frac{V}{k}$$

Ed ora altro più non resta che calcolare effettivamente questo integrale n^{plo} (16), nel che avremo una riprova che V è finito, e la formola (17) si muterà finalmente nella (I) § 48 che si tratta di dimostrare.

§ 50.

Calcolo dell'integrale n^{plo} V e forma definitiva della formola (I) § 48.

Il calcolo dell'integrale n^{plo} V si effettuerà riducendo, con un opportuno cangiamento di variabili, questo integrale ad avere limiti fissi. Per ciò, al posto delle n variabili reali $x_1, x_2 \dots x_n$, introdurremo come nuove n variabili (reali) in primo luogo le ν già introdotte $\mathfrak{U}, z_1, z_2 \cdots z_{\nu-1}$ (che variano per le (11), (12) fra i limiti fissi 0, 1) completate da altre $n-\nu = s$ le quali prenderemo gli argomenti $\psi_{\nu+1}, \psi_{\nu+2} \cdots \psi_n$ delle quantità $\varphi^{(\nu+1)}, \varphi^{(\nu+2)} \dots \varphi^{(n)}$, argomenti che si assumeranno fra 0 e 2π, cioè assoggettati alle limitazioni

$$(12) \qquad 0 \leq \psi_{\nu+1} < 2\pi, \quad 0 \leq \psi_{\nu+2} < 2\pi, \cdots 0 \leq \psi_n < 2\pi.$$

Per tal modo, ad ogni sistema di valori di $x_1, x_2 \cdots x_n$

appartenenti al nostro campo C, corrisponderà un solo sistema di valori delle nuove variabili

$$(19) \qquad (\mathfrak{U}, z_1, z_2, \dots z_{v-1}, \psi_{v+1} \dots \psi_n)$$

soddisfacenti alle limitazioni (11), (12) e (18). Se diamo invece un tale sistema delle nuove variabili, risulteranno perfettamente fissate le antiche $x_1, x_2 \dots x_n$ (o ciò che è lo stesso $\varphi^{(1)}, \varphi^{(2)} \dots \varphi^{(n)}$) solo quando tutti i corpi coniugati $K^{(1)} K^{(2)} \dots K^{(n)}$ sono immaginarii, cioè quando sia $r=0$, perchè allora di ciascuna $\varphi^{(i)}$ conosceremo insieme al modulo, l'argomento. Ma, se invece $r>0$, delle prime r quantità reali $\varphi^{(1)} \varphi^{(2)} \dots \varphi^{(r)}$ sono dati soltanto i valori assoluti e resta quindi libera la scelta fra due segni opposti per ciascuna; siccome però $\mathfrak{U}$ è positiva, e differisce dal prodotto $\varphi^{(1)} \varphi^{(2)} \dots \varphi^{(r)}$ solo per un fattore positivo, si hanno 2^{r-1} possibilità per $r>0$ ed una sola per $r=0$. Dunque: <u>ad ogni sistema delle nuove variabili (19) soddisfacenti alle limitazioni (11), (12) e (18) corrisponde un solo sistema per le antiche</u> $x_1, x_2 \dots x_n$, <u>entro il campo C, quando $r=0$ ed invece 2^{r-1} diversi se $r>0$.</u>

Ed ora, per effettuare la riduzione dell'integrale

$V = \int_{(C)} \cdots \int dx_1\, dx_2 \ldots dx_n$ alle nuove variabili (19), avremo da calcolare il determinante funzionale

$$(20) \qquad \frac{\partial(x_1, x_2 \cdots x_n)}{\partial(U, z_1, \cdots z_{\nu-1}, \psi_{\nu+1} \cdots \psi_n)},$$

ciò che faremo (fondandoci sulle note proprietà dei determinanti funzionali valide per variabili reali o complesse) per passaggi successivi. E in primo luogo passeremo per le intermediarie $\varphi^{(1)}, \varphi^{(2)} \cdots \varphi^{(n)}$, il cui determinante funzionale rispetto a $x_1 \cdots x_n$, a causa delle formole (7*), è precisamente il determinante [illegible] ha il valore sopra notato $NA\sqrt{\mathfrak{D}}$; dunque

$$(21) \qquad \frac{\partial(x_1, x_2, \cdots x_n)}{\partial(\varphi^{(1)}, \varphi^{(2)} \cdots \varphi^{(n)})} = \frac{1}{NA\sqrt{\mathfrak{D}}}$$

Alle prime ν quantità $\varphi^{(1)}, \varphi^{(2)} \cdots \varphi^{(\nu)}$ sostituiamo ora ν nuove variabili $R_1, R_2 \cdots R_\nu$ così definite che R_k sia il valore assoluto di $\varphi^{(k)}$ se $\varphi^{(k)}$ è reale (cioè per $k = 1, 2 \cdots r$) ed invece il quadrato del modulo quando $\varphi^{(k)}$ è complessa ($k = r+1, \ldots \nu$), e calcoliamo il determinante funzionale

$$\frac{\partial(\varphi^{(1)}, \varphi^{(2)}, \cdots \varphi^{(n)})}{\partial(R_1, R_2 \cdots R_\nu, \psi_{\nu+1} \cdots \psi_n)}$$

osservando che

$$\varphi^{(1)} = \pm R_1 \quad \varphi^{(2)} = \pm R_2 \ldots \varphi^{(r)} = \pm R_r$$

e per le nostre posizioni, ammesso che $\varphi^{(\nu+1)}, \varphi^{(\nu+2)} \ldots \varphi^{(n)}$

siano le rispettive complesse coniugate di $\varphi^{(r+1)}, \varphi^{(r+2)} \dots \varphi^{(v)}$, avremo

$$\varphi^{(r+1)} = \sqrt{R_{r+1}}\, e^{-i\psi_{v+1}}, \quad \varphi^{(v+1)} = \sqrt{R_{r+1}}\, e^{i\psi_{v+1}}$$
$$\varphi^{(r+2)} = \sqrt{R_{r+2}}\, e^{-i\psi_{v+2}}, \quad \varphi^{(v+2)} = \sqrt{R_{r+2}}\, e^{i\psi_{v+2}}$$
$$\dots\dots\dots\dots\dots\dots$$

Le variabili reali $\varphi^{(1)}, \varphi^{(2)} \dots \varphi^{(r)}$ non sono cangiate al più che nel segno, e per le complesse coniugate come $\varphi^{(r+1)}, \varphi^{(v+1)}$, a cui vengono sostituite R_{r+1}, ψ_{v+1} si ha

$$\frac{\partial(\varphi^{r+1}, \varphi^{(v+1)})}{\partial(R_{r+1}, \psi_{v+1})} = \begin{vmatrix} \frac{1}{2\sqrt{R_{r+1}}} e^{-i\psi_{v+1}}, & \frac{1}{2\sqrt{R_{r+1}}} e^{i\psi_{v+1}} \\ -i\sqrt{R_{r+1}}\, e^{-i\psi_{v+1}}, & i\sqrt{R_{r+1}}\, e^{i\psi_{v+1}} \end{vmatrix} = i$$

e risulta quindi

$$\frac{\partial(\varphi^{(1)}, \varphi^{(2)} \dots \varphi^{(n)})}{\partial(R_1, R_2 \dots R_r, \psi_{v+1} \dots \psi_n)} = \pm i^{n-v} = \pm i^s \quad (\text{cfr. § 16}). \tag{22}$$

Finalmente, al posto di $R_1, R_2 \dots R_v$, introduciamo le variabili definitive

$$U, z_1, z_2 \dots z_{v-1}$$

e calcoliamo il determinante funzionale

$$\frac{\partial(R_1, R_2 \dots R_v)}{\partial(U, z_1, z_2 \dots z_{v-1})}$$

Per questo osserviamo che si ha

$$U = R_1\, R_2 \dots R_v, \tag{23}$$

e pel modo come abbiamo definito, colle (8), le quan-

tità $y_1, y_2, \dots y_\nu$, risulta

$$y_h = \log R_h - C_h \log U \qquad (h = 1, 2, \dots \nu).$$

dove $C_h = \frac{1}{n}$ per $h = 1, 2, \dots r$ e pei rimanenti valori $r+1, \dots$ $\dots \nu$ di h è invece $C_h = \frac{2}{n}$.

Così abbiamo

$$(24) \qquad C_1 + C_2 + \dots + C_\nu = 1 \quad , \quad y_1 + y_2 + \dots y_\nu = 0$$

e da

$$\begin{cases} \log R_h = C_h \log U + y_h & h = 1, 2, \dots \nu-1 \\ \log R_\nu = C_\nu \log U - y_1 - y_2 \dots - y_{\nu-1} \end{cases}$$

si calcola subito

$$\frac{\partial(\log R_1, \log R_2, \dots \log R_\nu)}{\partial(\log U, y_1 \dots y_{\nu-1})} = \begin{vmatrix} C_1, & 1, & 0 & \dots & 0 \\ C_2, & 0, & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ C_{\nu-1}, & 0, & 0 & \dots & 1 \\ C_\nu, & -1, & -1 & \dots & -1 \end{vmatrix},$$

ove, addizionando all'ultima riga le $\nu-1$ precedenti con riguardo alla (24), risulta

$$\frac{\partial(\log R_1, \log R_2 \dots \log R_\nu)}{\partial(\log U, y_1 \dots y_{\nu-1})} = (-1)^{\nu-1},$$

od anche per la (23)

$$\frac{\partial(R_1, R_2, \dots R_\nu)}{\partial(U, y_1 \dots y_{\nu-1})} = (-1)^{\nu-1}$$

Questa formola, ove si osservi che per le (10)

$$\frac{\partial(\ldots)}{\partial(\ldots)} = \begin{vmatrix} l_{11} & l_{12} & \cdots & l_{1,v-1} \\ \cdot & \cdot & \cdots & \cdot \\ l_{v-1,1} & l_{v-1,2} & \cdots & l_{v-1,v-1} \end{vmatrix} = \mathcal{L}(\varepsilon_1, \varepsilon_2 \ldots \varepsilon_{v-1}),$$

si scrive anche

$$(24^*) \qquad \frac{\partial(R_1, R_2 \ldots R_v)}{\partial(U, z_1, z_2 \ldots z_{v-1})} = (-1)^{v-1}\mathcal{L}(\varepsilon_1, \varepsilon_2, \ldots \varepsilon_{v-1})$$

Ed ora, componendo con questa per moltiplicazione le (21), (22) superiori, troviamo pel determinante funzionale (20) il valore

$$(25) \qquad \frac{\partial(x_1, x_2, \ldots x_n)}{\partial(U, z_1, z_2, \cdots z_{v-1}, \psi_{v+1} \cdots \psi_n)} = \pm \frac{i^s \mathcal{L}(\varepsilon_1, \varepsilon_2, \cdots \varepsilon_{v-1})}{NA\sqrt{D}}.$$

Naturalmente questo valore (costante) è reale, come del resto si conferma da ciò che il numero fondamentale D del corpo è positivo o negativo secondo che s è pari o dispari. Il valore assoluto di questo determinante funzionale è dunque

$$\frac{\mathcal{L}(\varepsilon_1, \varepsilon_2 \cdots \varepsilon_{v-1})}{NA\sqrt{|D|}},$$

e per la formola di trasformazione degli integrali multipli è il fattore per cui bisogna moltiplicare ogni elemento

$$(a) \qquad dU\, dz_1\, dz_2 \cdots dz_{v-1}\, d\psi_{v+1} \cdots d\psi_v$$

dell'integrale trasformato per avere quelle corrispondente del primitivo

$$(b) \qquad dx_1\, dx_2 \cdots dx_n \, .$$

Da quanto poi abbiamo visto al principio del paragrafo risulta che ponendo

$$(26) \quad \begin{cases} \chi = 2^{r-1} & \text{se } r>0 \text{ (se vi sono corpi coniugati reali)} \\ \chi = 1 & \text{se } r=0. \text{ (se tutti i corpi coniugati sono immaginarii)} \end{cases}$$

ciascun elemento (a) va ripetuto χ volte per dare tutti gli elementi (b), ciascuno una volta sola. Avremo dunque

$$V = \int_{(C)} \cdots \int dx_1 \ldots dx_n = \frac{\chi \mathcal{L}}{NA\sqrt{|\mathfrak{D}|}} \int_0^1 dU \int_0^1 dz_1 \cdots \int_0^1 dz_{\nu-1} \int_0^{2\pi} d\varphi_{\nu+1} \cdots \int_0^{2\pi} d\varphi_n \, ,$$

cioè

$$(27) \qquad V = \frac{\chi \mathcal{L} (2\pi)^s}{NA\sqrt{|\mathfrak{D}|}} \, ,$$

od anche per le (26)

$$(28) \quad \begin{cases} V = \dfrac{2^{r-1}\pi^s \mathcal{L}}{NA\sqrt{|\mathfrak{D}|}} & \text{per } r>0 \\ V = \dfrac{2^s \pi^s \mathcal{L}}{NA\sqrt{|\mathfrak{D}|}} & \text{se } r=0 \end{cases}$$

La formola finale (17) del § precedente diventa così

$$\lim_{t=\infty} \left(\frac{T}{t}\right) = \frac{\chi \mathcal{L}(2\pi)^s}{k\sqrt{|\mathfrak{D}|}} \cdot \frac{1}{NA} \, ,$$

e se introduciamo la costante positiva

$$(29) \qquad g = \frac{\chi \mathcal{L}(2\pi)^s}{k\sqrt{|\mathfrak{D}|}}$$

indipendente dall'ideale A, col valore inerente soltanto al corpo $K(\theta)$:

$$(30)\qquad \begin{cases} g = \dfrac{2^{\nu+1}\pi^s \mathcal{L}(\varepsilon_1, \varepsilon_2 \cdots \varepsilon_{\nu-1})}{k\sqrt{|\mathfrak{D}|}} & \text{per } r>0 \\[2ex] g = \dfrac{(2\pi)^s \mathcal{L}(\varepsilon_1, \varepsilon_2 \cdots \varepsilon_{\nu-1})}{k\sqrt{|\mathfrak{D}|}} & \text{per } r=0 \end{cases}$$

ci troviamo ad avere stabilito la formola (I) enunciata nel teorema A) § 48.

§ 51

Conseguenze del teorema fondamentale - Doppia determinazione del numero h delle classi.

Dal teorema A) § 48 così dimostrato, assumendo per l'ideale arbitrario A l'ideale unità ($NA = 1$), risulta in particolare il significato della costante g come limite del rapporto $\frac{T}{t}$ per tutti gli ideali principali, cioè per gli ideali della classe principale. Ora è assai notevole che lo stesso valore g del $\lim\limits_{t=\infty}\left(\frac{T}{t}\right)$ si presenta in ogni altra classe H, e cioè sussiste il teorema:

α) Se H è una qualunque classe di ideali, e per ogni valore positivo arbitrario t della variabile reale t, si indica con T il numero degli ideali A della classe H, la cui norma non supera t

$$NA \leq t,$$

al crescere infinito di t il rapporto $\frac{T}{t}$ converge verso il limite g, indipendente dalla classe H:

$$(1) \qquad \lim_{t=\infty}\left(\frac{T}{t}\right)=g.$$

E infatti dalla classe inversa H prendiamo un qualunque ideale fisso M (un moltiplicatore). Se A è un ideale di H, sarà

$$(2) \qquad AM=(\alpha)$$

un ideale principale (α) divisibile per M; e viceversa da ogni ideale principale (α) divisibile per M segue la (2) con A ideale di H. Vi ha così corrispondenza biunivoca fra gli ideali principali (α), divisibili per M, e gli ideali A della classe H. Se però fra questi ultimi ci limitiamo a considerare quelli, in numero di T, che hanno $NA \leq t$, corrispondentemente per la (2) avremo

$$N(\alpha)=NA.N(M)\leq t\,N(M)$$

e se poniamo $t'=tN(M)$, crescerà t' all'infinito con t. Ma ora, dal teorema A) § 48, segue

$$\lim_{t=\infty}\left(\frac{T}{t'}\right)=\frac{g}{N(M)},$$

ossia $\lim_{t=\infty}\left(\frac{T}{t}\right)=g$, che è appunto la (I).

Ed ora consideriamo le h classi diverse

$$H_1 , H_2 , \cdots H_h$$

e denotiamo con T_i il numero degli ideali della classe H_i la cui norma non supera t; avremo per la (1)

$$\lim_{t=\infty} \left(\frac{T_i}{t}\right) = g \qquad i = 1, 2, \cdots h$$

Sommando e ponendo $T = T_1 + T_2 + \cdots + T_h$, è manifestamente T il numero di tutti i possibili ideali A con $NA \leq t$, e di qui il risultato fondamentale di Dedekind:

β) Se T denota il numero di tutti gli ideali diversi, la cui norma non supera il valore positivo arbitrario t, al crescere infinito di t, cresce anche T all'infinito, ma in guisa che il rapporto $\frac{T}{t}$ converge verso il limite determinato e finito (non nullo)

$$(II) \qquad \lim_{t=\infty} \left(\frac{T}{t}\right) = gh ,$$

dove h indica il numero delle classi.

Ed ora, se riusciremo a determinare lo stesso limite $\lim_{t=\infty}\left(\frac{T}{t}\right)$ per un'altra via, la formola (II) condurrà ad una prima determinazione del numero h delle classi. Questa via viene offerta appunto dalle proprietà della funzione $\zeta_K(s)$ di Dedekind, poichè dall'esistenza ora accertata del limite del rapporto $\frac{T}{t}$ seguirà

quella indicata alla fine del § 47 per

$$\lim_{s=1+0} \left\{(s-1)\zeta_K(s)\right\}$$

che si troverà eguale al primo, ed effettuato il prolungamento analitico di $\zeta_K(s)$, non sarà poi altro che il residuo di $\zeta_K(s)$ nel polo (del 1° ordine) $s=1$.

Per dimostrare questo, ricorriamo alla rappresentazione analitica (4) § 47 della $\zeta_K(s)$ sotto la forma della serie di Dirichlet

$$(3) \qquad \zeta_K(s) = \sum_m \frac{F(m)}{m^s} \qquad (R(s)>1)$$

dove m percorre tutti gli interi che sono norme di ideali esistenti, ed $F(m)$ è il numero degli ideali di norma $=m$. Se poniamo dunque $t=m$, pel significato stesso di T, sarà

$$T = F(1) + F(2) + \cdots + F(m),$$

e dalla formola (II) segue dunque per la nostra serie (3) di Dirichlet l'esistenza di

$$(4) \qquad \lim_{m=\infty} = \frac{F(1)+F(2)+\cdots+F(m)}{m} = gh.$$

Pensiamo ora numerati tutti gli ideali diversi

$$A_1,\ A_2 \cdots\cdots A_j \cdots,$$

e disposti per ordine di norme crescenti o stazionarie

$$m_1,\ m_2, \cdots\cdots m_j \cdots,$$

divisi dunque in tanti gruppi di egual norma, sicchè il primo gruppo consterà del solo ideale unità, il secondo di $F(2)$ ideali di norma $= 2$ (che può anche mancare se $F(2)=0$), e così via. Se poniamo $m = m_j$ avremo per lo meno j ideali di norma $\leq m$, cioè

$$j \leq F(1) + F(2) + \cdots + F(m).$$

Invece il numero degli ideali la cui norma non supera $\underline{m-1}$ sarà certo inferiore a j, perchè già A_j ha norma $m > m-1$, e di qui le limitazioni

$$F(1) + F(2) + \cdots + F(m-1) < j \leq F(1) + F(2) + \cdots + F(m),$$

a cui si può dare la forma

$$\frac{F(1)+F(2)+\cdots+F(m-1)}{m-1}\left(1-\frac{1}{m}\right) < \frac{j}{m_j} \leq \frac{F(1)+F(2)+\cdots+F(m)}{m}.$$

Ma qui le successioni a destra e a sinistra convergono, per la (4), verso lo stesso limite gh, e quindi è anche

$$(5) \qquad \lim_{j=\infty}\left(\frac{j}{m_j}\right) = gh.$$

Questo significa che, fissato un numero δ positivo arbitrario, si può prendere un indice j' tanto grande che si abbia

$$gh - \delta < \frac{j}{m_j} < gh + \delta \qquad \text{per } j \geq j',$$

cioè

$$\frac{gh-\delta}{j} < \frac{1}{m_j} < \frac{gh+\delta}{j} \qquad (j \geq j').$$

Per s reale >1 abbiamo quindi

$$(6)\qquad (gh-\delta)^s \sum_{j=j'}^{j=\infty} \frac{1}{j^s} < \sum_{j=j'}^{j=\infty} \frac{1}{m_j^s} < (gh+\delta)^s \sum_{j=j'}^{j=\infty} \frac{1}{j^s}.$$

Se, tenendo fisso δ e quindi j', moltiplichiamo queste diseguaglianze per $s-1$ e facciamo tendere s a 1, siccome per la (V) § 46 si ha

$$\lim_{s=1} \left\{ (s-1) \sum_{j=j'}^{j=\infty} \frac{1}{m_j^s} \right\} = \lim_{s=1} \left\{ (s-1)\zeta(s) \right\} = 1$$

a sinistra nella (6) il limite è $gh-\delta$, a destra $gh+\delta$, quindi se σ è un'altra quantità piccola a piacere, possiamo prendere $s-1$ così piccolo che da allora in poi

$$(s-1) \sum_{j=j'}^{j=\infty} \frac{1}{m_j^s}$$

differisca da gh per meno di $\delta+\sigma$. Ora, avendosi

$$\zeta_K(s) = \sum_{j=1}^{j=\infty} \frac{1}{m_j^s} = \sum_{j=1}^{j=j'-1} \frac{1}{m_j^s} + \sum_{j=j'}^{j=\infty} \frac{1}{m_j^s},$$

anche $(s-1)\zeta_K(s)$ differirà da gh per meno di $\delta+\sigma'$, con σ' piccolo a piacere. E siccome δ stesso è piccolo a piacere, se ne conclude

$$\lim_{s=1} \left\{ (s-1)\zeta_K(s) \right\} = gh,$$

ed abbiamo la formola finale (di Dedekind) che si trattava di stabilire:

$$(\text{III})\qquad h = \frac{1}{g} \lim_{s=1} \left\{ (s-1)\zeta_K(s) \right\}.$$

Così il numero h delle classi di ideali, per ogni corpo algebrico, risulta espresso quale limite di una serie infinita. Quanto alla sommazione della serie stessa, questa non si sa effettuare che in pochi casi particolari, nel caso dei corpi quadratici con formole date da Dirichlet per la teoria delle forme binarie quadratiche, per i corpi circolari da Kummer, per quelli cubici da Dedekind ecc.

In generale tale questione è intimamente legata alle proprietà aritmetiche ed algebriche del corpo in considerazione ed a quelle di corrispondenti funzioni trascendenti, quali le funzioni esponenziali, le ellittiche o modulari ecc.

§ 52

Trasformazione della formola (III) nel caso dei corpi quadratici col prolungamento analitico della $\zeta_D(s)$ al semipiano $\Re(s)>0$.

Nel caso dei corpi quadratici indicheremo con $\zeta_D(s)$ la funzione zèta di Dedekind, D avendo sempre il significato del numero fondamentale del corpo (cfr.

§ 32).

Tenendo conto dei risultati relativi agli ideali primi in questi corpi, comincieremo dal trasformare la formola che definisce $\zeta_{\mathfrak{D}}(s)$ nel semipiano $\mathcal{R}(s)>1$ in un'altra, colla quale la funzione stessa riesce analiticamente prolungata a tutto il semipiano $\mathcal{R}(s)>0$, come abbiamo fatto al § 46 per la $\zeta(s)$ di Riemann. Il processo dovuto a Dedekind, col quale si riesce a ottenere siffatto prolungamento, è il seguente.

Partiamo dalla seconda formola (§ 47 (II)), che definisce la funzione $\zeta_{\mathfrak{D}}(s)$ nel semipiano $\mathcal{R}(s)>1$ per prodotto infinito

$$(I) \qquad \zeta_{\mathfrak{D}}(s)=\prod_{P}\frac{1}{1-\frac{1}{(NP)^s}} \qquad (\mathcal{R}(s)>1);$$

ricordiamo che questo prodotto infinito in tutto l'interno di questo semipiano è incondizionatamente (ed uniformemente) convergente in senso stretto ed i singoli fattori corrispondono a tutti gli ideali primi P del corpo, ordinati in modo arbitrario.

Si è visto al § 32 che vi sono tre specie di questi ideali primi P a seconda della specie del numero primo p coordinato a P (incluso il caso $p=2$). Il 1° caso si dà quan-

do p entra in $\mathfrak{D}$ (è critico), ed allora

$$(p) = P^2 , \quad NP = p ;$$

il secondo quando p non entra in $\mathfrak{D}$, ma $\mathfrak{D}$ è residuo quadratico di $4p$, e allora

$$(p) = PP' , \quad NP = p ,$$

e i due ideali primi P, P' sono diversi (coniugati); il terzo infine quando p non divide $\mathfrak{D}$, e $\mathfrak{D}$ è non residuo di $4p$; in tal caso

$$(p) = P , \quad NP = p^2 .$$

Nel prodotto infinito (I) a destra poniamo insieme i fattori che provengono da ideali primi P appartenenti ad uno stesso numero primo p ordinario, e questi saranno ordinatamente nei tre casi

a) $\quad (1 - p^{-s})^{-1}$

b) $\quad (1 - p^{-s})^{-2}$

c) $\quad (1 - p^{-2s})^{-1}$

Per raccogliere questi tre casi in uno solo, Dedekind introduce il simbolo

$$(1) \qquad (\mathfrak{D}, p) ,$$

al quale attribuisce il valore $(\mathfrak{D}, p) = 0$ nel caso a), $(\mathfrak{D}, p) = +1$ in b), $(\mathfrak{D}, p) = -1$ in c).

Si osservi che, se p è dispari e non divide D, allora il valore di (D, p) non è altro che quello del simbolo di Legendre $\left(\frac{D}{p}\right)$. Conviene poi estendere la definizione del simbolo (1) anche al caso di un numero qualunque m composto, e se m si decompone in fattori primi, eguali o diversi: $m = p\,p'p''\ldots$, si porrà

$$(2) \qquad (D, m) = (D,p)(D,p')(D,p'')\ldots ;$$

e infine, per convenzione, si farà

$$(3) \qquad (D, 1) = 1.$$

È manifesto che questo simbolo soddisfa alla legge generale

$$(4) \qquad (D, m)\,(D, m') = (D, m\,m').$$

Ciò posto, i tre casi a), b), c) si raccoglieranno in questo solo che, in ogni caso, da un numero primo p proverrà a destra in (I) il prodotto

$$(1 - p^{-s})^{-1}\left(1 - (D,p)\,p^{-s}\right)^{-1},$$

e perciò la (I), avuto riguardo alla (4), potrà scriversi

$$\zeta_D(s) = \prod_p \left(\frac{1}{1 - \frac{1}{p^s}}\right) \cdot \prod_p \left(\frac{1}{1 - \frac{(D,p)}{p^s}}\right).$$

Il primo dei due prodotti infiniti non è altro che la $\zeta(s)$ di Riemann (§ 45 (III*)); quanto al secondo, se

si applica la trasformazione d'Eulero (I) § 44 col porre

$$f(n) = \frac{(\mathfrak{D}, n)}{n^s},$$

colla qual cosa, per la (4), restano soddisfatte le due condizioni fondamentali (A), (B) § 44, risulta trasformato nella serie $\sum_{n=1}^{n=\infty} \frac{(\mathfrak{D}, n)}{n^s}$, e la formola di definizione della $\zeta_{\mathfrak{D}}(s)$ (sempre nel semipiano $\mathcal{R}(s) > 1$) resta cangiata nella equivalente

$$\zeta_{\mathfrak{D}}(s) = \zeta(s) \cdot \sum_{n=1}^{n=\infty} \frac{(\mathfrak{D}, n)}{n^s} \qquad (\mathcal{R}(s) > 1).$$

Se nella serie a destra (che per $\mathcal{R}(s) > 1$ è assolutamente convergente) pensiamo i termini ordinati secondo $\underline{n}$ crescente, come è indicato nella sommazione, abbiamo una serie di Dirichlet (§ 45), che per ora sappiamo ammettere il semipiano $\mathcal{R}(s) > 1$ come semipiano di assoluta convergenza. Ma di più diciamo che essa converge condizionatamente, però uniformemente, entro la striscia $\mathcal{R}(s) = 0$, $\mathcal{R}(s) = 1$, e allora rappresenterà in tutto l'interno del semipiano $\mathcal{R}(s) > 0$ una funzione regolare della variabile complessa $\underline{s}$. Ciò ammesso, e ricordato che la $\zeta(s)$ esiste pure in tutto il detto semipiano (§ 46), ne risulterà che: <u>anche la $\zeta_{\mathfrak{D}}(s)$ è prolungabile analiticamente a tutto</u>

il detto semipiano e quivi definita dalla formola

$$(II) \qquad \zeta_{\mathfrak{D}}(s) = \zeta(s) \cdot \sum_{n=1}^{n=\infty} \frac{(\mathfrak{D}, n)}{n^s} \qquad (\mathfrak{R}(s) > 0).$$

Resta che proviamo l'effettiva convergenza uniforme della detta serie in ogni campo interno al semipiano $\mathfrak{R}(s) > 0$, per la qual cosa, secondo il lemma A) § 45 sulle serie di Dirichlet, basterà provare che per s reale e positivo la serie

$$(5) \qquad \sum_{1}^{\infty} \frac{(\mathfrak{D}, n)}{n^s}$$

è convergente.

Questo dedurremo dal teorema più generale seguente:

Se in una serie di Dirichlet $\sum_{1}^{\infty} \frac{a_n}{n^s}$, posto $A_n = a_1 + a_2 + \cdots + a_n$, le quantità A_n restano in modulo inferiori ad una quantità fissa A, la serie è convergente per ogni s reale positivo.

La dimostrazione in sostanza è già racchiusa in quella data al § 45 pel lemma A) citato (ove si ponga $s_0 = 0$). Si consideri infatti la somma $R_{m,p}$ di p termini consecutivi della serie dopo l'm^{mo}

$$R_{m,p} = \frac{a_{m+1}}{(m+1)^s} + \frac{a_{m+2}}{(m+2)^s} + \cdots + \frac{a_{m+p}}{(m+p)^s},$$

che si può scrivere (essendo $a_{m+k} = A_{m+k} - A_{m+k-1}$)

$$R_{m,p} = A_{m+1}\left\{\frac{1}{(m+1)^s} - \frac{1}{(m+2)^s}\right\} + A_{m+2}\left\{\frac{1}{(m+2)^s} - \frac{1}{(m+3)^s}\right\} + \cdots + A_{m+p-1}\left\{\frac{1}{(m+p-1)^s} - \frac{1}{(m+p)^s}\right\} + \frac{A_{m+p}}{(m+p)^s} - \frac{A_m}{(m+1)^s}.$$

Le differenze $\frac{1}{(m+k)^s} - \frac{1}{(m+k+1)^s}$ sono tutte positive, e tutte le A_n sono in modulo inferiori ad A, onde deducesi la limitazione

$$\left|R_{m,p}\right| < A\left\{\left(\frac{1}{(m+1)^s} - \frac{1}{(m+2)^s}\right) + \left(\frac{1}{(m+2)^s} - \frac{1}{(m+3)^s}\right) + \cdots + \left(\frac{1}{(m+p+1)^s} - \frac{1}{(m+p)^s}\right)\right\} + \frac{A}{(m+p)^s} + \frac{A}{(m+1)^s},$$

cioè

$$\left|R_{m,p}\right| < \frac{2A}{(m+1)^s},$$

e questa, per m abbastanza grande, è una quantità piccola a piacere (per qualunque p).

Per applicare questo al caso della serie (5), conviene porre $a_n = (D, n)$, dove dunque a_n è nullo oppure ± 1, e dimostrare che le somme A_n restano limitate, il che risulterà se proviamo che la somma di $|D|$ qualunque coefficienti consecutivi (D, n) è nulla. Ma siccome, se n non è primo con D, per la definizione stessa del simbolo, è $(D, n) = 0$, basterà considerare i soli valori di n primi con D. Se dunque D è pari, indi $= 4d$ (§ 14), i valori da considerarsi per n sono quelli dispari e primi con d; ma per questi è $(D, n) = \left(\frac{d}{n}\right)$ ed è ben noto che la

somma $\sum_n \left(\frac{d}{n}\right)$ dei simboli di Jacobi, estesa a un sistema completo di valori n primi con $4d$, è nulla (Dirichlet - Lezioni § 52, pag. 121). Si osservi che in ogni caso $(D, n) = (D, n')$, se $n \equiv n' \pmod{D}$. Se poi D è dispari, indi (§ 14) $D = d \equiv 1 \pmod 4$, si osservi che se n, n' sono due numeri congrui $\pmod D$ è anche $(D, n) = (D, n')$ come nel caso precedente. E infatti sia P il valore assoluto di D, e siano 2^ν, $2^{\nu'}$ le massime potenze del 2 che dividono rispettivamente n, n', onde

$$n = 2^\nu \cdot \mu, \quad n' = 2^{\nu'} \cdot \mu', \quad \text{con } \mu, \mu' \text{ dispari}$$

$$\text{e} \quad 2^\nu \cdot \mu \equiv 2^{\nu'} \cdot \mu' \pmod P.$$

Ora

$$(D, n) = (D, 2)^\nu (D, \mu),$$

e siccome

$$(D, 2) = \left(\frac{2}{P}\right), \; (D, \mu) = \left(\frac{D}{\mu}\right) = \left(\frac{\mu}{D}\right) = \left(\frac{\mu}{P}\right)$$

perchè $D \equiv 1 \pmod 4$, ne viene

$$(D, n) = \left(\frac{2}{P}\right)^\nu \left(\frac{\mu}{P}\right) = \left(\frac{n}{P}\right)$$

e similmente $(D, n') = \left(\frac{n'}{P}\right)$, per ciò da $n \equiv n' \pmod D$ segue $(D, n) = (D, n')$. Se allora facciamo percorrere ad $\underline{n}$ un sistema completo di $\varphi(P)$ numeri incongrui, e primi col modulo D (o P), e poniamo

$$S = \sum_n (\mathfrak{D}, n)$$

facilmente si vede che $S = 0$. Prendasi infatti un numero ν primo con $\underline{\mathfrak{D}}$ e tale che $(\mathfrak{D}, \nu) = -1$ (V^i Dirichlet § 52 pag. 117) e moltiplicando la precedente per $(\mathfrak{D}, \nu)$,

$$-S = \sum_n (\mathfrak{D}, \nu)(\mathfrak{D}, n) = \sum_n (\mathfrak{D}, \nu n) \quad \text{(per la (4))},$$

e siccome νn percorre con n un altro tale sistema completo, è dunque

$$-S = S\,, \quad S = 0 \qquad \text{c. d. d.}$$

Resta così provato che la serie infinita (5) di Dirichlet è convergente uniformemente in ogni regione interna al semipiano $R(s) > 0$, e rappresenta quindi ivi una funzione regolare della $\underline{s}$. In particolare questa sarà regolare nel punto $s = 1$, dove ha il valore

$$(6) \qquad \sum_n \frac{(\mathfrak{D}, n)}{n}\,,$$

ed anzi, dalla formola di Dedekind (III), vediamo che: <u>questo valore</u> $\sum_n \frac{(\mathfrak{D}, n)}{n}$ <u>è certo diverso da zero</u>, chè altrimenti diventando ivi $\zeta(s)$ infinita del 1° ordine, la $\zeta_{\mathfrak{D}}(s)$ non avrebbe in $s = 1$ singolarità alcuna, e la citata formola di Dedekind darebbe $h = 0$, ciò

che è assurdo. Il valore della serie infinita (6) è adunque il residuo della funzione $\zeta_D(s)$ nel polo del 1° ordine $s=1$, e la formola di Dedekind diventa nel caso attuale dei corpi quadratici:

$$k = \frac{1}{g} \sum_n \frac{(D,n)}{n} \;,$$

ove per la costante g dovremo sostituire il suo valore effettivo secondo le formole (30) § 50. Per questo occorre soddistinguere i due casi:

a) $D<0$, corpo quadratico immaginario

b) $D>0$, corpo quadratico reale.

a) In questo primo caso i valori che competono ai numeri r, s, ν, k delle formole (30) § 50 sono

$$r=0 \;, \quad s=1 \;, \quad \nu=1$$

e generalmente (§ 14): $k=2$, salvo $k=6$ per $D=-3$, $k=4$ per $D=-4$. Quanto alla costante $L = L(\varepsilon_1, \varepsilon_2 \cdots \varepsilon_{\nu-1})$ che ivi figura, facilmente vediamo che qui è da prendere $L=1$ perchè, pur restando applicabile l'analisi del § 50 nel caso attuale $n=2$, $D<0$ le variabili z_1, $z_2 \ldots z_{\nu-1}$ spariscono e la costante L introdotta nella (24*) § 50, come valore del determinante funzionale $\dfrac{\partial(R_1, R_2 \ldots R_\nu)}{\partial(u, z_1, \ldots z_{\nu-1})}$, qui, avendosi $\nu=1$, si riduce alla deriva-

ta semplice $\frac{dR_1}{dU}$, e poichè dalle (23) § 50 è $R_1 = U$, resta appunto $\mathcal{L} = 1$. E allora la seconda delle (30) § 50 ci dà generalmente

$$g = \frac{\pi}{\sqrt{-D}},$$

e invece $g = \frac{\pi}{4}$ per $D = -4$, $g = \frac{\pi}{3\sqrt{3}}$ per $D = -3$. Lasciando dunque da parte questi due ultimi casi eccezionali, la formola di Dedekind per h diventa

$$(III) \qquad h = \frac{\sqrt{-D}}{\pi} \sum_{(n)} \frac{(D,n)}{n} \qquad (D < 0, \neq -3, -4)$$

b) Se $D > 0$ abbiamo $r = 2$, $s = 0$, $v = 2$. Esiste una sola unità fondamentale è data da $\frac{T + U\sqrt{D}}{2}$, dove T, U sono i <u>più piccoli interi positivi</u> che soddisfano all'equazione di Pell: $T^2 - DU^2 = 4$, e di unità ridotte si dànno le due sole ± 1, onde dobbiamo porre nella prima delle (30) § 50:

$$v = 2, \quad s = 0, \quad \mathcal{L} = \log \varepsilon, \quad k = 2$$

e resta $g = \frac{\log \varepsilon}{\sqrt{D}}$, e perciò la formola finale

$$(IV) \qquad h = \frac{\sqrt{D}}{\log\left(\frac{T + U\sqrt{D}}{2}\right)} \sum_{(n)} \frac{(D,n)}{n} \qquad (D > 0)$$

Con queste formole (III) e (IV) è conseguita una prima parte dello scopo e cioè si è espresso il numero h delle classi, in un corpo quadratico, sotto una forma che

dipende unicamente dal numero fondamentale D del corpo. Ma ora si può domandare di sommare effettivamente la serie $\sum_{(n)} \frac{(D,n)}{n}$ del secondo membro e di porre il suo valore sotto una forma che ponga in evidenza la natura del numero h come intero positivo. Tutto ciò si consegue sostituendo alla valutazione della serie quella di un opportuno integrale definito, e facendo uso dei valori di certe particolari somme finite, che Gauss incontrò nelle ricerche sulle equazioni per la divisione del circolo, ed ora si dicono somme di Gauss.

§ 53.

Somme di Gauss e loro prime proprietà.

Il primo e più semplice esempio di una somma S di Gauss si ha pel caso di un numero primo n dispari, ponendo

$$\varepsilon = e^{\frac{2\pi i}{n}},$$

e distinguendo le $n-1$ radici (primitive) n^{me} dell'unità

$$\varepsilon, \varepsilon^2, \varepsilon^3 \dots \varepsilon^{n-1}$$

in due gruppi, di $\frac{n-1}{2}$ termini ciascuno, appartenendo al primo gruppo le potenze con esponente $\underline{a}$ residuo quadratico (mod n), al secondo quelle con esponente $\underline{b}$ non residuo; la relativa somma S di Gauss è

$$S = \sum \varepsilon^a - \sum \varepsilon^b ,$$

che possiamo anche scrivere

$$S = \sum_s \left(\frac{s}{n}\right) e^{\frac{2s\pi i}{n}} ,$$

dove l'indice variabile $\underline{s}$ percorre un sistema completo di resti (mod n), escluso lo zero. Se si osserva poi che si ha

$$\sum \varepsilon^a + \sum_1 \varepsilon^b = 1$$

si può dare a S anche la forma

$$S = 1 + 2 \sum_1 \varepsilon^a ,$$

o ciò che è lo stesso

$$(1) \qquad S = \sum_{s=0}^{s=n-1} e^{s^2 \frac{2\pi i}{n}} ;$$

dove ora $\underline{s}$ percorre tutti i valori di un sistema completo di resti (mod n). Mediante semplici considerazioni aritmetiche, si trova che il quadrato di S è il numero intero razionale

$$S^2 = (-1)^{\frac{n-1}{2}} \cdot n ,$$

onde segue

$$S = \pm \sqrt{n} \quad , \quad \text{se} \quad n \equiv 1 \pmod 4$$

$$S = \pm i\sqrt{n} \quad , \quad \text{se} \quad n \equiv 3 \pmod 4 ;$$

ma la decisione sul segno da scegliere in queste formole ha presentato a Gauss stesso gravi difficoltà. Qui risulterà la decisione dalle ricerche più generali seguenti.

Le somme generali di Gauss che passiamo a considerare, per n intero qualunque positivo, sono quelle definite dalla espressione

$$\sum_s e^{s^2 \cdot \frac{2h\pi i}{n}} ,$$

dove h è un intero fisso qualunque, e, nella sommazione, s percorre un sistema completo di resti (mod n). Questa somma dipende unicamente dai due interi h, n, e si indicherà con

$$\varphi(h, n) = \sum_s e^{s^2 \cdot \frac{2h\pi i}{n}} ; \tag{2}$$

noi ne troveremo l'effettivo valore, almeno per quei casi che occorrono nel seguito. Ma conviene prima segnalare alcune semplici proprietà delle somme di Gauss, che serviranno ad una riduzione del problema.

a) Si ha sempre

$$(a) \qquad \varphi(h,n) = \varphi(h',n)\,, \quad \text{se} \quad h \equiv h' \pmod n,$$

perchè allora $e^{\frac{2h'\pi i}{n}} = e^{\frac{2h\pi i}{n}}$.

b) Se l'intero $\underline{a}$ è primo con n, risulta

$$(b) \qquad \varphi(ha^2,n) = \varphi(h,n).$$

Questo è manifesto osservando che cangiando $\underline{s}$ in $\underline{as}$ anche $\underline{as}$ percorre con $\underline{s}$ un sistema completo di resti (mod n), e d'altronde questo cangiamento a destra nella (2) equivale a cangiare h in ha^2.

c) Se n, n' sono due interi qualunque (positivi) primi fra loro, sussiste la formola

$$(c) \qquad \varphi(hn',n)\cdot\varphi(hn,n') = \varphi(h,nn').$$

E difatti, formando il primo membro della (c) colla (2), si ottiene

$$\varphi(hn',n)\cdot\varphi(hn,n') = \sum_{s,s'} e^{s^2\frac{2hn'\pi i}{n} + s'^2\frac{2hn\pi i}{n'}} = \sum_{s,s'} e^{(s^2n'^2+s'^2n^2)\frac{2h\pi i}{nn'}}$$

dove nella sommazione $\underline{s}$ percorre un sistema completo di resti (mod n) ed $\underline{s'}$ un tale sistema (mod n'). Ma avendosi

$$s^2n'^2 + s'^2n^2 \equiv (sn'+s'n)^2 \pmod{nn'},$$

se si pone

$$r = sn' + s'n\,,$$

e si considera che n, n' sono primi fra loro, ne segue che r percorre un sistema completo di resti (mod $n.n'$), e per ciò

$$\varphi(hn', n)\cdot\varphi(hn, n') = \sum_r e^{r^2\frac{2h\pi i}{nn'}} = \varphi(h, nn'), \quad \text{c. d. d.}$$

d) Se $\underline{b}$ è un numero qualunque positivo, si ha

$$(d) \qquad \varphi(bh, bn) = b\,\varphi(h, n).$$

Per la (2) è infatti

$$\varphi(bh, bn) = \sum_s e^{s^2\frac{2h\pi i}{n}},$$

dove $\underline{s}$ percorre un sistema completo di resti (mod bn), e per ciò $\underline{b \text{ volte}}$ un sistema completo di resti (mod n), ciò che dimostra la (d).

Fondandosi su queste proprietà, si può ridurre il calcolo delle somme di Gauss al caso di $\underline{n}$ primo e di $h = 1$. A noi qui basterà calcolare $\varphi(1, n)$ per n qualunque e $\varphi(h, n)$ per $\underline{n}$ dispari, ed $\underline{h}$ primo con n.

§ 54.

Determinazione di $\varphi(1, n)$ secondo Kronecker.

Fra i vari metodi che si hanno pel calcolo delle somme di Gauss, scegliamo quello che fa uso della

teoria dell'integrazione nel campo complesso e conduce alla determinazione di $\varphi(1,n) = \sum_s e^{s^2 \frac{2\pi i}{n}}$ col procedimento seguente di Kronecker. Si consideri la funzione

$$(1) \qquad f(z) = \frac{e^{\frac{2\pi i}{n} z^2}}{e^{2\pi i z} - 1},$$

uniforme in tutto il piano complesso, con poli del 1° ordine in tutti i punti interi dell'asse reale

$$z = 0, \quad z = \pm 1, \quad z = \pm 2, \dots,$$

in generale nel polo $z = k$ (k intero) col residuo:

$$\frac{1}{2\pi i} e^{\frac{2\pi i}{n} k^2}.$$

Nel piano complesso si tracci il rettangolo contenuto fra le due rette verticali (parallele all'asse y):

$$x = 0, \quad x = \frac{n}{2}$$

e le due orizzontali (parallele all'asse delle x)

$$y = -h, \quad y = h,$$

dove $\underline{h}$ è una quantità positiva arbitraria, che faremo poi crescere infinitamente.

Nell' <u>interno</u> di questo rettangolo la nostra funzione $f(z)$ presenta i poli

$$z = 1, 2, 3, \dots s,$$

ove $\underline{s}$ è il massimo intero <u>inferiore</u> a $\frac{n}{2}$, e sul con-

torno si ha il polo $z=0$, poi eventualmente, per n pari, il polo $z=\frac{n}{2}$. Per escluderli, tracciamo coi rispettivi centri in $z=0$, $z=\frac{n}{2}$ due circoli di raggio r, che si farà poi tendere a zero, e togliamo dall'area rettangolare i due semicerchi ad essa interni. Il campo così formato [si descriva la figura] contiene nel suo interno i poli $z=1, 2, \dots s$ ed il suo contorno consta di una parte rettilinea, che indicheremo con L, e dalle due semicirconferenze tracciate con raggio $= r$. L'integrale $\int f(z)\,dz$ esteso al contorno completo, percorso nel verso diretto, sarà eguale alla somma dei residui, moltiplicata per $2\pi i$, cioè a

$$\sum_{k=1}^{k=s} e^{\frac{2\pi i}{n}k^2},$$

che possiamo anche scrivere

$$\frac{1}{2}\sum_{k=1}^{k=s}\left\{e^{\frac{2\pi i}{n}k^2}+e^{\frac{2\pi i}{n}(n-k)^2}\right\}.$$

Ora l'integrale esteso al contorno si decompone nella parte estesa alla porzione rettilinea L, e nelle due estese alle semicirconferenze, percorse nel verso opposto a quello positivo delle rotazioni. Se percorriamo queste semicirconferenze σ_1, σ_2 nel verso di-

retto, avremo dunque

$$(2) \quad \int_{\mathcal{L}} f(z)\,dz = \int_{\sigma_1} f(z)\,dz + \int_{\sigma_2} f(z)\,dz + \frac{1}{2}\sum_{k=1}^{k=s}\left(e^{\frac{2\pi i}{n}k^2} + e^{\frac{2\pi i}{n}(n-k)^2}\right).$$

Facciamo ora tendere a zero il raggio r di σ_1, σ_2, e dimostriamo che il secondo membro di questa formola ha un limite determinato e finito, che sarà quindi anche il limite del primo. Se l'integrale $\int_{\sigma_1} f(z)\,dz$ si scrive

$$\int_{\sigma_1} z f(z) \cdot \frac{dz}{z}$$

e si osserva che, al decrescere di r il prodotto $z f(z)$ converge verso il residuo di $f(z)$ in $z = 0$, cioè verso $\frac{1}{2\pi i}$, mentre $\int_{\sigma_1} \frac{dz}{z} = i\int_0^{\pi} d\theta = \pi i$, ne segue subito

$$\lim_{r=0} \int_{\sigma_1} f(z)\,dz = \frac{1}{2}.$$

Nel medesimo modo vediamo che se n è dispari, cioè $\frac{n}{2}$ non è un polo di $f(z)$, allora

$$\lim_{r=0} \int_{\sigma_2} f(z)\,dz = 0\,;$$

quando invece n è pari, e $z = \frac{n}{2}$ è un polo di $f(z)$ col residuo $= \frac{1}{2\pi i} \cdot e^{\frac{2\pi i}{n}\left(\frac{n}{2}\right)^2}$, allora

$$\lim_{r=0} \int_{\sigma_2} f(z)\,dz = \frac{1}{2}\, e^{\frac{2\pi i}{n}\left(\frac{n}{2}\right)^2}.$$

In ogni caso adunque il secondo membro della (2) ha per limite, quando r tende a zero, precisamente la metà della somma $\varphi(1, n)$ di Gauss, e quindi

$$2\lim_{r=0} \int_{\mathcal{L}} f(z)\,dz = \varphi(1, n).$$

Dell'integrale esteso alla parte rettilinea L esaminiamo in primo luogo le due parti estese ai tratti orizzontali

$$y = -h \, , \qquad J_1 = \int_0^{\frac{n}{2}} f(x - ih)\, dx$$

$$y = +h \, , \qquad J_2 = \int_{\frac{n}{2}}^0 f(x + ih)\, dx \, ,$$

e dimostriamo che ambedue convergono a zero, al crescere infinito di h. Per questo si osservi che il modulo di $f(z)$ è dato da

$$f(z) = \frac{e^{-\frac{4\pi}{n} xy}}{\sqrt{\left(e^{-2\pi y} - 1\right)^2 + 4 \operatorname{sen}^2 \pi x \, e^{-2\pi y}}} \, ,$$

e possiamo scrivere la limitazione

$$|f(z)| \leq \frac{e^{-\frac{4\pi}{n} xy}}{\left| e^{-2\pi y} - 1 \right|} \; ;$$

ne segue che

$$|f(z)| \leq \frac{e^{\frac{4\pi h}{n} x}}{e^{2\pi h} - 1} \, , \quad \text{sul lato} \quad y = -h$$

$$|f(z)| \leq \frac{e^{-\frac{4\pi h}{n} x}}{1 - e^{-2\pi h}} \, , \quad \text{sul lato} \quad y = +h$$

Dunque per i moduli di J_1, J_2 avremo

$$|J_1| \leq \frac{1}{e^{2\pi h} - 1} \int_0^{\frac{n}{2}} e^{\frac{4\pi h}{n} x}\, dx \leq \frac{n}{4\pi h}$$

$$|J_2| \leq \frac{1}{1 - e^{-2\pi h}} \int_0^{\frac{n}{2}} e^{-\frac{4\pi h}{n} x}\, dx \leq \frac{n}{4\pi h} \, ,$$

onde si vede appunto che, al crescere infinito di h, gli integrali J_1, J_2 convergono a zero.

I rimanenti integrali rettilinei si scindono in

quattro, due che diciamo J_3, J_4 estesi ai due tratti della retta $x = \frac{n}{2}$, e gli altri due J_5, J_6 ai due tratti della retta $x=0$; abbiamo

$$J_3 = i\int_{-h}^{-r} f\left(\tfrac{n}{2}+iy\right)dy \quad , \quad J_4 = i\int_{r}^{h} f\left(\tfrac{n}{2}+iy\right)dy$$

$$J_5 = i\int_{h}^{r} f(iy)\,dy \quad , \quad J_6 = i\int_{-r}^{-h} f(iy)\,dy$$

Cangiando in J_3 e in J_6 la variabile d'integrazione y in $-y$, risulta

$$J_3 + J_4 = i\int_{r}^{h}\left\{f\left(\tfrac{n}{2}+iy\right)+f\left(\tfrac{n}{2}-iy\right)\right\}dy$$

$$J_5 + J_6 = -i\int_{r}^{h}\left\{f(iy)+f(-iy)\right\}dy \,.$$

Ora, tenendo conto delle due identità

$$\frac{1}{t-1} + \frac{1}{t^{-1}-1} = -1$$

$$\frac{t}{(-1)^n t-1} + \frac{t^{-1}}{(-1)^n t^{-1}-1} = (-1)^n$$

si trova subito che si ha

$$f(iy)+f(-iy) = -e^{-\frac{2\pi i}{n}y^2}$$

$$f\left(\tfrac{n}{2}+iy\right)+f\left(\tfrac{n}{2}-iy\right) = i^{-n}\, e^{-\frac{2\pi i}{n}y^2} ,$$

e per ciò

$$J_3+J_4+J_5+J_6 = \left(i+i^{1-n}\right)\int_{r}^{h} e^{-\frac{2\pi i}{n}y^2}\,dy.$$

Si è visto che, facendo crescere h infinitamente, e insieme tendere r a zero, questa espressione conver

ge verso $\frac{1}{2}\varphi(1,n)$, ed abbiamo quindi intanto

$$\varphi(1,n) = 2(i+i^{1-n})\int_0^\infty e^{-\frac{2\pi i}{n}y^2}dy.$$

Indicando con $\sqrt{n}$ il valore positivo della radice quadrata di n eseguiamo nell'integrale a destra il cangiamento di variabile

$$y = u\sqrt{n}\,,$$

onde avremo

$$(3)\qquad \varphi(1,n) = 2\sqrt{n}\,(i+i^{1-n})\int_0^\infty e^{-2\pi i u^2}du.$$

Questa formola vale per qualunque n, in particolare per $n=4$, dove si ha direttamente

$$\varphi(1,4) = \sum_{s=0}^{s=3} e^{\frac{\pi i}{2}s^2} = i^0 + i^1 + i^4 + i^9 = 2(1+i)$$

e ne segue intanto

$$(4)\qquad \int_0^\infty e^{-2\pi i u^2}du = \frac{1-i}{4}.$$

[Si osservi che scindendo qui il reale dall'immaginario, col cangiare la variabile u d'integrazione in $\frac{x}{\sqrt{2\pi}}$, e raddoppiando, si hanno i valori dei ben noti integrali definiti

$$\int_{-\infty}^{+\infty}\cos(x^2)\,dx = \int_{-\infty}^{+\infty}\operatorname{sen}(x^2)\,dx = \sqrt{\frac{\pi}{2}}\ ].$$

Se si sostituisce il valore (4) nella (3), si ottiene infine il valore cercato per la somma di Gauss $\varphi(1,n)$

$$(I)\qquad \varphi(1,n) = \sqrt{n}\,\frac{i+i^{1-n}}{1+i}\,;$$

e se si suddistingue in riguardo del carattere di n (mod 4) risulta rispettivamente

$$\varphi(1,n) = (1+i)\sqrt{n} \quad , \text{ per } n \equiv 0 \pmod 4$$
$$\varphi(1,n) = \sqrt{n} \quad , \;\text{"}\; n \equiv 1 \pmod 4$$
$$\varphi(1,n) = 0 \quad , \;\text{"}\; n \equiv 2 \pmod 4$$
$$\varphi(1,n) = +i\sqrt{n} \quad , \;\text{"}\; n \equiv 3 \pmod 4 .$$

In generale, riunendo il terzo ed il quarto caso di n dispari, si può scrivere

$$\text{(II)} \qquad \varphi(1,n) = i^{\left(\frac{n-1}{2}\right)^2}\sqrt{n} \qquad \left(n \equiv 1 \pmod 2\right)$$

§ 55

I valori delle somme di Gauss in generale.

Servendoci delle formole sopra ottenute per $\varphi(1,n)$, e delle proprietà generali delle somme di Gauss (§ 53), si può facilmente trovare il valore di qualunque $\varphi(h,n)$. A noi basterà considerare due casi principali, e cioè: a) il caso di n numero primo p dispari ed h non divisibile per p, b) il caso di n numero dispari P privo di fattori quadrati, ed h primo con P.

a) Nel caso di n numero primo dispari p, la (II) dà

$$\varphi(1,p) = i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p} \,,$$

e se $\underline{h}$ non è divisibile per p, possiamo scrivere (§ 52)

$$\varphi(h,p) = \sum_s \left(\frac{s}{p}\right) e^{\frac{2hs\pi i}{p}},$$

dove $\underline{s}$ percorre un sistema completo di resti (mod p), escluso lo zero. Ponendo $hs = s'$, anche $\underline{s}'$ percorre un tale sistema completo, ed avendosi $\left(\frac{s}{p}\right) = \left(\frac{h}{p}\right)\left(\frac{s'}{p}\right)$, si può scrivere

$$\varphi(h,p) = \left(\frac{h}{p}\right) \sum_{s'} \left(\frac{s'}{p}\right) e^{\frac{2s'\pi i}{p}} = \left(\frac{h}{p}\right) \varphi(1,p)$$

e si ha quindi per la formola richiesta

$$(\text{II}^*) \qquad \varphi(h,p) = \left(\frac{h}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p} \qquad (h \not\equiv 0 \ (\text{mod}\ p)).$$

Si osservi che, nella deduzione di queste formole per le somme di Gauss, non si è fatto uso del teorema di reciprocità nella teoria dei residui quadratici; ed anzi ora si può trarre, con Gauss, una nuova dimostrazione di questo teorema fondamentale. Applicando la (II*) a due numeri primi dispari diversi p, q risulta

$$\varphi(q,p) = \left(\frac{q}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}$$

$$\varphi(p,q) = \left(\frac{p}{q}\right) i^{\left(\frac{q-1}{2}\right)^2} \sqrt{q},$$

indi

$$\varphi(q,p) \cdot \varphi(p,q) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) i^{\left(\frac{p-1}{2}\right)^2 + \left(\frac{q-1}{2}\right)^2} \sqrt{pq}.$$

Ma per la proprietà (c) § 53 delle somme di Gauss è

$$\varphi(q,p)\,\varphi(p,q)=\varphi(1,pq),$$

e per la (II)

$$\varphi(1,pq)=i^{\left(\frac{pq-1}{2}\right)^2}\sqrt{pq},$$

onde dal confronto risulta

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=i^{\left(\frac{pq-1}{2}\right)^2-\left(\frac{p-1}{2}\right)^2-\left(\frac{q-1}{2}\right)^2}$$

D'altra parte avendosi

$$\frac{pq-1}{2}\equiv\frac{p-1}{2}+\frac{q-1}{2}\pmod 2$$

indi

$$\left(\frac{pq-1}{2}\right)^2\equiv\left(\frac{p-1}{2}+\frac{q-1}{2}\right)^2\equiv\left(\frac{p-1}{2}\right)^2+\left(\frac{q-1}{2}\right)^2+2\,\frac{p-1}{2}\,\frac{q-1}{2}\pmod 4,$$

ne viene

$$i^{\left(\frac{pq-1}{2}\right)^2-\left(\frac{p-1}{2}\right)^2-\left(\frac{q-1}{2}\right)^2}=i^{2\frac{p-1}{2}\cdot\frac{q-1}{2}}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

e la formola finale

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

che è la nota espressione del teorema di reciprocità.

b) Sia ora $n=P$ un numero (positivo) dispari, privo di fattori quadrati, ed $\underline{h}$ primo con P. Risolvendo P in fattori primi abbiasi

$$P=p_1\,p_2\cdots p_r$$

con $p_1, p_2, \dots p_r$ numeri primi diversi, e pongasi

$$\frac{P}{p_1}=P_1\,,\quad\frac{P}{p_2}=P_2\,,\;\dots\;\frac{P}{p_r}=P_r\,,$$

onde sarà P_i primo con p_i. Dalla proprietà (c) § 53 ab-

biamo

$$\varphi(h,P) = \varphi(h, p_1 P_1) = \varphi(hP_1, p_1)\cdot\varphi(hp_1, P_1),$$

e colla medesima formola (C)

$$\varphi(hp_1, P_1) = \varphi(hp_1 p_2, p_3 \cdots p_r)\cdot\varphi(hP_2, p_2),$$

per cui

$$\varphi(h,P) = \varphi(hP_1, p_1)\,\varphi(hP_2, p_2)\,\varphi(hp_1p_2, p_3\cdots p_r).$$

Applicando ripetutamente questa formola ricorrente si arriva alla generale

$$(1) \qquad \varphi(h,P) = \varphi(hP_1, p_1)\,\varphi(hP_2, p_2)\cdots\varphi(hP_r, p_r),$$

che scriviamo

$$(2) \qquad \varphi(h,P) = \prod_{j=1}^{j=n} \varphi(hP_j, p_j).$$

Questa vale anche se h non è primo con P, tale ipotesi non essendo stata utilizzata nella deduzione. Ma se ora supponiamo h primo con P, cioè non divisibile nè per p_1, nè per p_2, ... nè per p_r ed applichiamo la (II^*), troviamo:

$$\varphi(h,P) = \sqrt{P}\,\prod_j \left(\frac{hP_j}{p_j}\right) i^{\Sigma\left(\frac{p-1}{2}\right)^2},$$

formola che può scriversi

$$\varphi(h,P) = \left(\frac{h}{P}\right)\sqrt{P}\cdot i^{\Sigma\left(\frac{p-1}{2}\right)^2} \prod \left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right),$$

il prodotto riferendosi alle combinazioni due a due dei numeri primi $p_1, p_2 \cdots p_r$. Ma si ha, pel teorema di

reciprocità:

$$\Pi\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right)=(-1)^{\sum \frac{p-1}{2}\cdot\frac{p'-1}{2}}=i^{2\sum \frac{p-1}{2}\cdot\frac{p'-1}{2}},$$

e quindi

$$\varphi(h,P)=\left(\frac{h}{P}\right)\sqrt{P}\; i^{\left(\sum \frac{p-1}{2}\right)^2}$$

In fine, poichè

$$\frac{P-1}{2}\equiv\sum \frac{p-1}{2} \pmod 2, \quad \left(\frac{P-1}{2}\right)^2\equiv\left(\sum \frac{p-1}{2}\right)^2 \pmod 4,$$

la formola cercata per $\varphi(h,P)$ diventa

$$\text{(III)} \qquad \varphi(h,P)=\left(\frac{h}{P}\right) i^{\left(\frac{P-1}{2}\right)^2}\cdot\sqrt{P}$$

e comprende naturalmente la (II^*), relativa al caso $P=p$.

A questa formola (III) si può dare un'altra forma, risalendo alla (2), coll'esprimere ciascun fattore a destra con

$$\varphi(hP_j,p_j)=\sum_{s_j}\left(\frac{s_j}{p_j}\right)e^{s_j\frac{2hP_j\pi i}{p_j}}=\sum_{s_j}\left(\frac{P_j s_j}{p_j}\right)e^{s_j\frac{2h\pi i}{p_j}},$$

onde la (2) diventa

$$\varphi(h,P)=\sum\left(\frac{P_1 s_1}{p_1}\right)\left(\frac{P_2 s_2}{p_2}\right)\cdots\left(\frac{P_r s_r}{p_r}\right)e^{\frac{2h\pi i}{P}(P_1 s_1+P_2 s_2+\cdots+P_r s_r)},$$

dove $s_1, s_2, \cdots s_r$ percorrono rispettivamente un sistema completo di resti (escluso lo zero) rispetto ai moduli $p_1, p_2, \cdots p_r$. Ora abbiamo

$$\left(\frac{P_1 s_1+P_2 s_2+\cdots+P_r s_r}{P}\right)=\left(\frac{P_1 s_1}{p_1}\right)\left(\frac{P_2 s_2}{p_2}\right)\cdots\left(\frac{P_r s_r}{p_r}\right),$$

e d'altronde il numero

$$s = P_1 s_1 + P_2 s_2 + \cdots + P_r s_r$$

percorre un sistema completo di $\varphi(F)$ resti primi con P. Dunque:

Quando h è primo con P, si ha

$$\varphi(h,P) = \sum_s \left(\frac{s}{P}\right) e^{s\frac{2h\pi i}{P}},$$

come nel caso di P primo.

La formola (III) si può scrivere adunque anche sotto la forma seguente

$$\text{(IV)} \qquad \sum_s \left(\frac{s}{P}\right) e^{s\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right) i^{\left(\frac{P-1}{2}\right)^2} \cdot \sqrt{P}.$$

È importante osservare che questa formola resta vera anche quando h non è primo con P, purchè si faccia la nuova convenzione che il simbolo di Jacobi $\left(\frac{\mu}{P}\right)$ significhi lo zero quando μ non è primo con P, dopo di che le proprietà fondamentali del simbolo stesso continuano a sussistere. Ora il calcolo sopra eseguito dà sempre

$$\sum_s \left(\frac{s}{P}\right) e^{s\frac{2h\pi i}{P}} = \prod_j \left(\sum_j \left(\frac{P_j s_j}{p_j}\right) e^{s_j \frac{2h\pi i}{p_j}} \right),$$

ma in tal caso uno almeno dei fattori a destra si

annulla poichè se h è divisibile pel numero primo p si ha $e^{\frac{2h\pi i}{p}} = 1$, indi

$$\sum \left(\frac{s}{p}\right) e^{\frac{2h\pi i}{p}} = \sum \left(\frac{s}{p}\right) = 0$$

e la (IV) sussiste ancora perchè $\left(\frac{h}{p}\right) = 0$.

In ogni caso adunque sarà applicabile la formola (IV) e, per la nuova convenzione sul simbolo di Jacobi, potremo far scorrere s per un sistema completo di resti (mod P), compresi quelli non primi con P.

§ 56

Riduzione della serie $\sum \frac{(D,n)}{n}$ a un integrale definito. Caso $D \equiv 1 \pmod 4$.

Dopo queste premesse sulle somme di Gauss, ritorniamo alle formole finali del § 52 per la determinazione del numero h delle classi nel corpo quadratico, dove si trattava ancora di eseguire la sommazione della serie

$$(1) \qquad S = \sum_{n=1}^{n=\infty} \frac{(D,n)}{n}.$$

Questa ridurremo al calcolo di un integrale definito, partendo dalla formola elementare

$$\frac{1}{n} = \int_0^1 x^{n-1}\, dx,$$

onde la (1) può scriversi

$$(1') \qquad S = \sum_{n=1}^{n=\infty} \int_0^1 \frac{dx}{x} (\mathfrak{D}, n) x^n .$$

Indicando con k un numero intero positivo, che si farà poi crescere all'infinito, prendiamo la somma dei primi $k|\mathfrak{D}|$ termini della (1'), facendo percorrere ad $\underline{n}$ i valori

$$n = r|\mathfrak{D}| + s \begin{cases} r = 0, 1, 2, \dots k-1 \\ s = 1, 2 \dots \dots |\mathfrak{D}| \end{cases}$$

Ricordando (§ 52) che $(\mathfrak{D}, n) = (\mathfrak{D}, s)$ (perchè $n \equiv s$ (mod $\mathfrak{D}$)), e denotando la detta somma (finita) con S_k, avremo

$$(2) \qquad S_k = \int_0^1 \frac{dx}{x} \cdot \sum_{s=1}^{s=|\mathfrak{D}|} (\mathfrak{D}, s) x^s \cdot \sum_{r=0}^{r=k-1} x^{r \cdot |\mathfrak{D}|} .$$

Ma si ha

$$\sum_{r=0}^{r=k-1} x^{r|\mathfrak{D}|} = \frac{1 - x^{k|\mathfrak{D}|}}{1 - x^{|\mathfrak{D}|}} ,$$

e ponendo

$$(3) \qquad F(x) = \sum_{s=1}^{s=|\mathfrak{D}|} (\mathfrak{D}, s) x^s = (\mathfrak{D}, 1) x + (\mathfrak{D}, 2) x^2 + \dots + (\mathfrak{D}, |\mathfrak{D}|) x^{|\mathfrak{D}|}$$

questa $F(x)$ è un polinomio di grado $|\mathfrak{D}|-1$, perchè $(\mathfrak{D}, |\mathfrak{D}|) = 0$; esso inoltre si annulla per $x = 0$, come è evidente, ma anche per $x = 1$, a causa della proprietà segnalata al § 52

$$\sum_s (\mathfrak{D}, s) = 0 .$$

La formula (2) diventa così

$$S_k = \int_0^1 \frac{F(x)}{x(1-x^{|D|})}\left(1-x^{k|D|}\right)dx,$$

che può decomporsi in

$$(4) \qquad S_k = \int_0^1 \frac{F(x)\,dx}{x(1-x^{|D|})} - \int_0^1 \frac{F(x).\,x^{k|D|}}{x(1-x^{|D|})}\,dx.$$

La seconda parte, quando facciamo crescere k all'infinito, converge a zero, perchè annullandosi, come si è visto, $F(x)$ per $x=0$ e per $x=1$, nell'intervallo fra 0 e 1 la frazione $\frac{F(x)}{x(1-x^{|D|})}$ rimane limitata, e per ciò, indicando con A il massimo del valore assoluto di detta frazione, quello dell'integrale sarà inferiore ad

$$A\int_0^1 x^{k|D|}\,dx = \frac{A}{k|D|+1}$$

valore che, al crescere infinito di k, converge a zero. E siccome $S = \lim_{k=\infty} S_k$, abbiamo trasformato il valore S della nostra serie in quello dell'integrale definito

$$(I) \qquad S = \sum_n \frac{(D,n)}{n} = \int_0^1 \frac{F(x)\,dx}{x(1-x^{|D|})}.$$

La funzione sotto il segno è una funzione razionale della x che, in tutto l'intervallo d'integrazione (limiti inclusi), è sempre finita, e non resta più che

compiere l'effettiva integrazione, colle regole del calcolo integrale (per logaritmi ed archi tangenti), per avere S e quindi di $\underline{h}$ sotto forma chiusa.

Nel calcolo effettivo è da distinguere secondo che il numero fondamentale D è pari o dispari, ed il più semplice è il secondo caso nel quale adunque (§ 14)

$$(5) \qquad D = d \equiv 1 \pmod 4 ;$$

noi ci limiteremo a trattare questo caso, le formole degli altri casi avendo una struttura del tutto analoga.

Indichiamo con P il valore assoluto di D, talchè, secondo la (5), avremo

$P \equiv 3 \pmod 4$, $D = -P$, se il corpo quadratico è immaginario

$P \equiv 1 \pmod 4$, $D = P$, se il corpo quadratico è reale.

Ricordiamo inoltre, dal § 5?, che è sempre in questo caso

$$(D, s) = \left(\frac{s}{P}\right),$$

e perciò la funzione $F(x)$, data dalla (3) si può ora scrivere

$$(6) \qquad F(x) = \sum_{s=1}^{s=P-1} \left(\frac{s}{P}\right) x^s .$$

Ed ora andiamo a decomporre la frazione razionale

$$(7) \qquad \frac{F(x)}{x(1-x^P)}$$

sotto il segno integrale nella (I) in frazioni semplici. Posto

$$\varepsilon = e^{\frac{2\pi i}{P}}$$

le radici di $x^P - 1 = 0$ sono date da

$$\varepsilon^\alpha \quad \text{per} \quad \alpha = 0, 1, 2, \dots P-1,$$

e la decomposizione in frazioni semplici della (7) dà

$$\frac{F(x)}{x(1-x^P)} = -\frac{1}{P}\sum_{\alpha=1}^{\alpha=P-1} \frac{F(\varepsilon^\alpha)}{x-\varepsilon^\alpha},$$

dove è da omettere il termine $\alpha = 0$ perchè $F(1) = 0$. Ma per la (6)

$$F(\varepsilon^\alpha) = \sum_s \left(\frac{s}{P}\right) e^{s\frac{2\alpha\pi i}{P}}$$

per $\alpha \neq 0$ è precisamente una somma di Gauss e il suo valore, per la (IV) § 56, è

$$F(\varepsilon^\alpha) = \left(\frac{\alpha}{P}\right) i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P},$$

e sostituendo nella (I) risulta dunque

$$(8) \qquad S = -\frac{i^{\left(\frac{P-1}{2}\right)^2}}{\sqrt{P}} \sum_{\alpha=1}^{\alpha=P-1} \left(\frac{\alpha}{P}\right) \int_0^1 \frac{dx}{x - e^{\frac{2\pi i\alpha}{P}}}.$$

Resta da calcolare il valore dell'integrale definito $\int_0^1 \frac{dx}{x-e^{\frac{2\pi i\alpha}{P}}}$, ciò che può farsi per via elementare come segue. Per δ compreso fra $\underline{0}$ e $\underline{2\pi}$ calcoliamo

$$\int_0^1 \frac{dx}{x-e^{i\delta}} = \int_0^1 \frac{x - e^{-i\delta}}{(x-\cos\delta)^2 + \operatorname{sen}^2\delta}\, dx =$$

$$= \int_0^1 \frac{x-\cos\delta}{(x-\cos\delta)^2+\operatorname{sen}^2\delta}\,dx + i\operatorname{sen}\delta\int_0^1 \frac{dx}{(x-\cos\delta)^2+\operatorname{sen}^2\delta},$$

e siccome gli integrali indefiniti sono

$$\int \frac{x-\cos\delta}{(x-\cos\delta)^2+\operatorname{sen}^2\delta}\,dx = \frac{1}{2}\log\left\{(x-\cos\delta)^2+\operatorname{sen}^2\delta\right\}$$

$$\operatorname{sen}\delta\int \frac{dx}{(x-\cos\delta)^2+\operatorname{sen}^2\delta} = \operatorname{arctg}\left(\frac{x-\cos\delta}{\operatorname{sen}\delta}\right),$$

risulta

$$\int_0^1 \frac{dx}{x-e^{i\delta}} = \log\left(2\operatorname{sen}\frac{\delta}{2}\right) + i\left\{\operatorname{arc\,tg}\left(\operatorname{tg}\tfrac{1}{2}\delta\right)+\operatorname{arc\,tg}(\cot.\delta)\right\}$$

gli archi tangenti essendo presi fra $-\frac{\pi}{2}$ e $+\frac{\pi}{2}$. Ne risulta che, tanto quando δ è fra $\underline{0}$ e $\underline{\pi}$, come quando è fra π e 2π, abbiamo

$$(9) \qquad \int_0^1 \frac{dx}{x-e^{i\delta}} = \log\left(2\operatorname{sen}\frac{\delta}{2}\right) + \frac{i}{2}(\pi-\delta).$$

Sostituendo nella (8), troviamo

$$S = -\frac{i^{\left(\frac{P-1}{2}\right)^2}}{\sqrt{P}} \sum_{\alpha=1}^{\alpha=P-1}\left(\frac{\alpha}{P}\right)\left\{\log\left(2\operatorname{sen}\frac{\alpha\pi}{P}\right) + i\left(\frac{\pi}{2}-\frac{\alpha\pi}{P}\right)\right\},$$

e questa può ancora semplificarsi ricordando che $\sum\left(\frac{\alpha}{P}\right)=0$, e per ciò $\sum\left(\frac{\alpha}{P}\right)\log 2 = 0$, $\sum\left(\frac{\alpha}{P}\right)\frac{\pi}{2} = 0$. Resta così in definitiva

$$(10) \qquad S = -\frac{i^{\left(\frac{P-1}{2}\right)^2}}{\sqrt{P}} \sum_{\alpha}\left(\frac{\alpha}{P}\right)\left\{\log\operatorname{sen}\left(\frac{\alpha\pi}{P}\right) - i\,\frac{\alpha\pi}{P}\right\},$$

dove l'immaginario nel secondo membro, essendo S reale, dovrà necessariamente sparire.

Per compiere la riduzione, conviene ora separare

i due casi del corpo quadratico immaginario e di quello reale, e per calcolare h si adopererà nel primo caso la formola (III) del § 52, nel secondo invece la (IV), col sostituirvi per $\sum \frac{(\mathfrak{D},n)}{n}$ il valore calcolato dalla (10).

§ 57.

Separazione del caso del corpo quadratico immaginario e del corpo reale – Formole definitive per $\mathfrak{D} \equiv 1 \pmod 4$

a) Cominciando dal caso del corpo quadratico immaginario, abbiasi

$$\mathfrak{D} = -P, \quad P \equiv 3 \pmod 4, \quad \text{indi} \quad \left(\frac{P-1}{2}\right)^2 \equiv 1 \pmod 4,$$

e la formola (10) per S diventerà

$$S = -\frac{i}{\sqrt{P}} \sum_\alpha \left(\frac{\alpha}{P}\right) \left\{ \log \operatorname{sen}\left(\frac{\alpha\pi}{P}\right) - i\,\frac{\alpha\pi}{P} \right\}$$

che, per essere S reale, si separa nelle due

$$S = -\frac{\pi}{P\sqrt{P}} \sum_\alpha \alpha \left(\frac{\alpha}{P}\right) \tag{11}$$

$$\sum \left(\frac{\alpha}{P}\right) \log \operatorname{sen}\left(\frac{\alpha\pi}{P}\right) = 0 \,. \tag{12}$$

Quest'ultima si può verificare direttamente osservando che $P-\alpha$ percorre, come α, i valori $1, 2, 3, \ldots P-1$ e perciò

$$\sum_\alpha \left(\frac{\alpha}{P}\right) \log \operatorname{sen}\left(\frac{\alpha\pi}{P}\right) = \sum_\alpha \left(\frac{P-\alpha}{P}\right) \log \operatorname{sen}\left(\frac{(P-\alpha)\pi}{P}\right) = \sum \left(\frac{P-\alpha}{P}\right) \log \operatorname{sen}\left(\frac{\pi\alpha}{P}\right) =$$

$$= (-1)^{\frac{P-1}{2}} \sum_\alpha \left(\frac{\alpha}{P}\right) \log \operatorname{sen}\left(\frac{\pi\alpha}{P}\right),$$

onde, essendo $\frac{P-1}{2}$ dispari, segue la (12). Ed ora, sostituendo il valore (11) per S nella (III) § 52, risulta

$$(13) \qquad h = -\frac{1}{P} \sum_\alpha \alpha \left(\frac{\alpha}{P}\right),$$

nella quale intanto è posto in evidenza che h è un numero razionale. Ma di più ora possiamo trasformarla in guisa che apparisca la specie di h, come numero intero. Per questo scindiamo la sommazione rispetto ad α nei valori di $\alpha' < \frac{P}{2}$, e nei rimanenti complementari $P-\alpha'$, che sono invece maggiori di $\frac{P}{2}$. Così abbiamo

$$\sum_\alpha \alpha \left(\frac{\alpha}{P}\right) = \sum_{\alpha'=1}^{\alpha'=\frac{P-1}{2}} \alpha' \left(\frac{\alpha'}{P}\right) + \sum_{\alpha'=1}^{\alpha'=\frac{P-1}{2}} (P-\alpha') \left(\frac{P-\alpha'}{P}\right);$$

e siccome da $P \equiv 3 \pmod 4$ segue

$$\left(\frac{P-\alpha'}{P}\right) = -\left(\frac{\alpha'}{P}\right),$$

abbiamo

$$(14). \quad \sum_\alpha \alpha \left(\frac{\alpha}{P}\right) = 2 \sum_{\alpha'=1}^{\alpha'=\frac{P-1}{2}} \alpha' \left(\frac{\alpha'}{P}\right) - P \sum_{\alpha'=1}^{\alpha'=\frac{P-1}{2}} \left(\frac{\alpha'}{P}\right).$$

Ma anche i numeri $2\alpha'$, $P-2\alpha'$, inferiori tutti a P ed ii congeni, coincidono in altro ordine cogli α, e per ciò si ha anche -

$$\sum_{\alpha}' \alpha \left(\frac{\alpha}{P}\right) = \sum_{\alpha'} 2\alpha' \left(\frac{2\alpha'}{P}\right) + \sum_{\alpha'} \left(\frac{P-2\alpha'}{P}\right)(P-2\alpha') =$$

$$= 2\left(\frac{2}{P}\right)\sum_{\alpha'} \alpha' \left(\frac{\alpha'}{P}\right) - \frac{2}{P}\sum_{\alpha'} \left(\frac{\alpha'}{P}\right)(P-2\alpha'),$$

ovvero

$$\left(\frac{2}{P}\right)\sum_{\alpha} \alpha \left(\frac{\alpha}{P}\right) = 4\sum_{\alpha'} \alpha' \left(\frac{\alpha'}{P}\right) - P\sum_{\alpha'} \left(\frac{\alpha'}{P}\right).$$

Sottraendo questa dalla (14) moltiplicata per 2, si elimina $\sum_{\alpha'} \alpha' \left(\frac{\alpha'}{P}\right)$, e resta

$$\left\{2 - \left(\frac{2}{P}\right)\right\}\sum_{\alpha} \alpha \left(\frac{\alpha}{P}\right) = -P\sum_{\alpha'} \left(\frac{\alpha'}{P}\right),$$

indi sparisce dalla (13) il divisore P e si ottiene

$$h = \frac{\sum_{\alpha'=1}^{\alpha'=\frac{P-1}{2}} \left(\frac{\alpha'}{P}\right)}{2 - \left(\frac{2}{P}\right)}.$$

Siccome $P \equiv 3 \pmod 4$, potremo avere $P \equiv 7 \pmod 8$, ovvero $P \equiv 3 \pmod 8$; nel primo caso resta semplicemente

$$(15) \qquad h = \sum_{\alpha'=1}^{\alpha'=\frac{P-1}{2}} \left(\frac{\alpha'}{P}\right) \quad \text{per } P \equiv 7 \pmod 8,$$

nel secondo invece

$$(15^*) \qquad h = \frac{1}{3}\sum_{\alpha'=1}^{\alpha'=\frac{P-1}{2}} \left(\frac{\alpha'}{P}\right) \quad \text{per } P \equiv 3 \pmod 8 \ (P > 3).$$

Nel primo caso la (15) pone in evidenza che h è un intero, il quale però inoltre sarà certamente positivo. Si può quindi concludere: _Per avere il numero h delle classi per un corpo quadratico immaginario di determinan-_

te $D = -P \equiv 1 \pmod 4$, si considerino i numeri α' primi con P e giacenti nell'intervallo $\left(1, \frac{P-1}{2}\right)$ e si osservi per quanti di essi il simbolo $\left(\frac{\alpha'}{P}\right)$ di Jacobi riceve il valore $+1$ e per quanti il valore -1. Il numero dei primi è sempre maggiore di quello dei secondi e l'eccesso dà il numero h delle classi se $D \equiv 1 \pmod 8$ ed il suo triplo se $D \equiv 5 \pmod 8$.

In particolare, se P è un numero primo $p \equiv 3 \pmod 4$ segue che fra i numeri

$$1, 2, 3, \dots \frac{p-1}{2} \quad (*)$$

vi sono più residui quadratici che non residui, e l'eccesso dà il numero h delle classi per $D = -p$ ovvero il triplo di h, secondo che $D \equiv 1$ o $D \equiv 3 \pmod 8$. Questo singolare teorema, enunciato per induzione da Jacobi, venne così confermato da queste ricerche d'aritmetica analitica di Dirichlet.

b) Prendiamo ora in secondo luogo il caso del corpo quadratico reale, ove

$$D = +P \equiv 1 \pmod 4\ , \quad \left(\frac{P-1}{2}\right)^2 \equiv 0 \pmod 4,$$

(*) Quando $p \equiv 1 \pmod 4$, fra i numeri $1, 2, 3, \dots \frac{p-1}{2}$ vi sono tanti residui quanti non residui, perchè $\sum_{\alpha}\left(\frac{\alpha}{p}\right) = \sum_{\alpha'}\left(\frac{\alpha'}{p}\right) + \sum\left(\frac{p-\alpha'}{p}\right) = 2\sum\left(\frac{\alpha'}{p}\right) = 0.$

e la (10) diventa

$$S = -\frac{1}{\sqrt{P}} \sum_{\alpha} \left(\frac{\alpha}{P}\right) \left\{ \log \operatorname{sen}\left(\frac{\alpha\pi}{P}\right) - i\,\frac{\alpha\pi}{P} \right\},$$

che ora si sdoppia nelle due

$$(16) \qquad S = -\frac{1}{\sqrt{P}} \sum_{\alpha} \left(\frac{\alpha}{P}\right) \log \operatorname{sen}\left(\frac{\alpha\pi}{P}\right)$$

$$(16^*) \qquad \sum_{\alpha} \alpha \left(\frac{\alpha}{P}\right) = 0\,,$$

la seconda delle quali si verifica subito osservando che si ha

$$\sum_{\alpha} \alpha\left(\frac{\alpha}{P}\right) = \sum_{\alpha} (P-\alpha)\left(\frac{P-\alpha}{P}\right) = \sum_{\alpha} (P-\alpha)\left(\frac{-\alpha}{P}\right) = \sum_{\alpha} (P-\alpha)\left(\frac{\alpha}{P}\right) \quad (\text{perchè } P \equiv 1 \pmod 4),$$

e siccome $\sum_{\alpha} \left(\frac{\alpha}{P}\right) = 0$, così vale anche la (16*).

Quanto alla (16), distinguiamo i $\varphi(P)$ numeri primi con P in due classi di $\frac{1}{2}\varphi(P)$ numeri ciascuna, che diremo $\underline{a}$ e $\underline{b}$, secondo che

$$\left(\frac{a}{P}\right) = +1 \quad \text{o} \quad \left(\frac{b}{P}\right) = -1\,;$$

la (16) diventa così

$$S = \frac{1}{\sqrt{P}} \log \frac{\prod_b \operatorname{sen}\left(\frac{b\pi}{P}\right)}{\prod_a \operatorname{sen}\left(\frac{a\pi}{P}\right)}$$

e sostituendo nella (IV) § 52, avremo pel numero delle classi la formola

$$(17) \qquad h = \frac{1}{\log\left(\frac{T+U\sqrt{P}}{2}\right)} \cdot \log \frac{\prod_b \operatorname{sen}\left(\frac{b\pi}{P}\right)}{\prod_a \operatorname{sen}\left(\frac{a\pi}{P}\right)}\,.$$

Qui però, a differenza di quanto accadeva pel corpo immaginario, non è più messo in evidenza il carattere

di h come numero intero, ed occorre per ciò un'ulteriore trasformazione della formola. Il quoziente $\frac{\prod_b \operatorname{sen}\left(\frac{b\pi}{P}\right)}{\prod_a \operatorname{sen}\left(\frac{a\pi}{P}\right)}$ è un'unità nel corpo delle radici P^{me} della unità, col quale il corpo quadratico per $D = P$ sta nella singolare relazione, secondo la (17), che $\left(\frac{T+U\sqrt{D}}{2}\right)^h = \varepsilon^h$ eguaglia la detta unità nel corpo circolare.

Noi ci siamo qui limitati per brevità, nella ricerca del numero h delle classi di un corpo quadratico, al caso $D \equiv 1 \pmod 4$. Per gli altri casi, eseguendo le effettive integrazione, si trovano risultati perfettamente analoghi. Nel caso del determinante negativo (corpo immaginario) il numero h delle classi dipende dal modo di distribuzione negli otto ottanti della circonferenza dei punti $e^{\frac{2\pi i a}{2}}$, $e^{\frac{2\pi i b}{2}}$, e, nel caso di D positivo (corpo reale), dalla relazione che l'unità fondamentale ε del corpo ha con certe unità del corpo circolare.

§ 58.

La funzione ζ di Dedekind pel corpo circolare $k(\sqrt[m]{1})$ (m primo), estesa al semipiano $\mathcal{R}(s) > 0$.

Come nel caso dei corpi quadratici, così anche in quello dei corpi circolari delle radici m^{me} dell'unità (m qualunque), si conosce la legge degli ideali primi e si riesce facilmente a cangiare la formola che definisce la zèta di Dedekind nel semipiano $\mathcal{R}(s) > 1$ in una altra che la prolunga analiticamente a tutto il semipiano $\mathcal{R}(s) > 0$. Essendoci limitati, pei corpi circolari, a studiare, nel § 43, la legge di distribuzione degli ideali primi nel corpo circolare $k(\varepsilon)$ generato dalla radice m^{ma} dell'unità $\varepsilon = e^{\frac{2\pi i}{m}}$, per m primo dispari, noi effettueremo per questo caso il detto prolungamento analitico della funzione zèta di Dedekind, che indicheremo con $\zeta_m(s)$.

Partiamo anche qui dalla formola di definizione (II) § 47 della $\zeta_m(s)$ per prodotto infinito:

$$(1) \qquad \zeta_m(s) = \prod_P \frac{1}{1 - \frac{1}{(NP)^s}} \qquad (\mathcal{R}(s) > 1)$$

esteso a tutti gli ideali primi P del corpo. Ricordiamo

(§ 42) che l'unico numero primo critico $\underline{m}$ dà luogo ad un solo ideale primo (μ), $\mu = 1-\varepsilon$, di cui $\underline{m}$ è la potenza $(m-1)^{\text{ma}}$ ed è $N(\mu) = m$; invece ogni altro numero primo p (compreso $p=2$), se $\underline{f}$ è l'esponente cui appartiene (mod m), si decompone in $\frac{m-1}{f} = e$ ideali primi diversi:

$$(p) = P_1 P_2 \dots P_e ,$$

ciascuno di grado f, cioè con $NP = p^f$. E allora nel prodotto infinito (1), incondizionatamente convergente per $\mathcal{R}(s) > 1$, isoliamo il fattore $\frac{1}{1-\frac{1}{m^s}}$ che corrisponde al numero primo critico $\underline{m}$, e raggruppiamo gli altri a seconda dell'esponente f cui appartiene il numero primo $\underline{p}$ coordinato all'ideale P; così avremo:

$$(2) \qquad \zeta_m(s) = \frac{1}{1-\frac{1}{m^s}} \prod_p \frac{1}{\left(1-\frac{1}{p^s}\right)^e} .$$

Ora, presa una radice primitiva g (mod m), per ogni numero $\underline{n}$, non divisibile per $\underline{m}$, indichiamo in generale con $\underline{n'}$ il suo indice preso nella base g, sicchè

$$n \equiv g^{n'} \pmod{m}.$$

Siccome $\underline{p}$ appartiene all'esponente f, il suo indice p' avrà con $m-1$ il massimo comun divisore $\frac{m-1}{f} = e$, e se con $\underline{\omega}$ indichiamo una radice primitiva della equazione binomia

$$(3) \qquad x^{m-1} = 1\,,$$

tutte le radici di questa saranno date da

$$(4) \qquad \alpha = 1,\ \omega,\ \omega^2,\ \dots\ \omega^{m-2},$$

mentre $\omega^{p'}$ sarà una radice primitiva dell'altra equazione binomia

$$(5) \qquad x^f = 1\,,$$

le cui radici saranno tutte nella serie

$$(5^*) \qquad \alpha^{p'} = 1,\ \omega^{p'},\ \omega^{2p'} \dots \omega^{(m-2)p'},$$

e ciascuna vi si troverà ripetuta uno stesso numero di volte $= e$. Da questa osservazione risulta immediatamente l'identità

$$(1-x^f)^e = \prod_\alpha (1-\alpha^{p'}x)\,,$$

dove nel prodotto a destra α percorre gli $m-1$ valori (4). Ponendo in questa identità $x = \frac{1}{p^s}$, ne viene

$$\left(1-\frac{1}{p^{fs}}\right)^e = \prod_\alpha \left(1-\frac{\alpha^{p'}}{p^s}\right),$$

ed ora sostituendo nella (2), possiamo raccogliere i fattori che corrispondono a tenere fisso α, mentre p percorre tutti i numeri primi non divisibili per m. Designando con $\mathfrak{L}_\alpha(s)$ il corrispondente prodotto infinito

$$(5) \qquad \mathfrak{L}_\alpha(s) = \prod_p \frac{1}{1-\dfrac{\alpha^{\mathrm{ind}\,p}}{p^s}}\,,$$

la (2) si cangia nell'altra

$$(6) \qquad \zeta_m(s) = \frac{\mathcal{L}_1(s)}{1-\frac{1}{m^s}} \cdot \mathcal{L}_\omega(s)\,\mathcal{L}_{\omega^2}(s)\cdots\mathcal{L}_{\omega^{m-2}}(s).$$

È facile vedere che il primo fattore a destra $\frac{\mathcal{L}_1(s)}{1-\frac{1}{m^s}}$ non è altro che la $\zeta(s)$ di Riemann, poichè esprimendo per prodotti infiniti secondo la (5)

$$\frac{\mathcal{L}_1(s)}{1-\frac{1}{m^s}} = \frac{1}{1-\frac{1}{m^s}} \prod_p{}' \frac{1}{1-\frac{1}{p^s}},$$

dove l'accento nel prodotto infinito indica che p percorre tutti i numeri primi escluso m, mentre appunto $\zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}}$, incluso m.

Se ora al prodotto infinito ( ) applichiamo la trasformazione d'Eulero § 44, col porre per qualsiasi intero n

$$\begin{cases} f(n) = \dfrac{\alpha^{\operatorname{ind} n}}{n} & \text{quando } n \not\equiv 0 \pmod m \\ f(n) = 0 & \text{per } n \equiv 0 \pmod m \end{cases}$$

si vede súbito che le condizioni del § 44 (essendo $R(s)>1$) sono soddisfatte e ne risulta quindi per le funzioni $\mathcal{L}_\alpha(s)$ quest'altra espressione per serie

$$(7) \qquad \mathcal{L}_\alpha(s) = \sum_n \frac{\alpha^{\operatorname{ind} n}}{n^s} \quad (n \not\equiv 0 \pmod m)$$ nel semipiano $R(s)>1$.

In particolare per $\alpha = 1$

$$\mathcal{L}_1(s) = \sum{}' \frac{1}{n^s},$$

l'accento nella somma indicando che qui n percorre tut

ti gli interi positivi con esclusione dei multipli di m. Ne risulta nuovamente la relazione notata

$$(8) \qquad \mathcal{L}_1(s) = \left(1 - \frac{1}{m^s}\right) \zeta(s) \, ,$$

perchè avendosi

$$\zeta(s) = \sum \frac{1}{n^s}$$

dove qui n percorre tutti gli interi positivi, se decomponiamo questa somma in due parti la prima corrispondente ai valori di n non divisibili per m, l'altra a quelli divisibili, risulta manifestamente

$$\zeta(s) = \mathcal{L}_1(s) + \sum_n \frac{1}{(mn)^s} = \mathcal{L}_1(s) + \frac{1}{m^s}\zeta(s) \, ,$$

onde la (8).

Ritorniamo alla (6), che scriviamo ora

$$(I) \qquad \zeta_m(s) = \zeta(s) \prod_\alpha{}' \mathcal{L}_\alpha(s) \, , \qquad (\alpha \neq 1)$$

dove s'intende che nel prodotto (finito) a destra α percorre tutte le radici (4) della (3), con esclusione di $\alpha = 1$.

Ora se nella serie (7), che definisce $\mathcal{L}_\alpha(s)$ dapprima nel semipiano $\mathcal{R}(s) > 1$, pensiamo i termini ordinati secondo i valori crescenti di n, abbiamo una serie di Dirichlet, che nell'interno di quel semipiano converge assolutamente ed uniformemente. Ma ora diciamo che quando $\alpha \neq 1$ ciascuna di queste $m-2$

serie di Dirichlet

$$\mathcal{L}_{\omega}(s),\ \mathcal{L}_{\omega^2}(s),\ \dots \mathcal{L}_{\omega^{m-2}}(s)$$

continua a convergere uniformemente (non più assolutamente) in ogni campo interno alla striscia compresa fra le parallele $\mathcal{R}(s)=0$, $\mathcal{R}(s)=1$. Questo è una facile conseguenza del teorema sulle serie di Dirichlet al § 52, che ci ha servito alla ricerca analoga nel caso dei corpi quadratici, e del fatto che se n percorre un sistema completo di $m-1$ numeri incongrui (mod m), con esclusione dello zero, l'indice di n percorre i numeri $0, 1, 2, \dots m-2$, e per ciò, essendo $\alpha \neq 1$

$$\sum \alpha^{\mathrm{ind}\, n} = \frac{\alpha^{m-1}-1}{\alpha-1} = 0 .$$

Dopo ciò è chiaro che, se nella (I) poniamo

$$f(s) = \prod_{\alpha} \mathcal{L}_{\alpha}(s) \qquad (\alpha \neq 1),$$

questa $f(s)$ è una funzione regolare di s in tutto il semipiano $\mathcal{R}(s)>0$. Dunque la formola (I), avendo già effettuato, al § 46, il prolungamento analitico al semipiano $\mathcal{R}(s)>0$ della $\zeta(s)$ Riemanniana, dà il prolungamento cercato della $\zeta_m(s)$ relativa al campo circolare:

$$(I^*) \qquad \zeta_m(s) = \zeta(s)\cdot f(s) \qquad (\mathcal{R}(s)>0).$$

Ma ritorniamo alla formola di Dedekind (§ 51 (III))

pel calcolo del numero h delle classi

$$(9)\qquad gh = \lim_{s=1}\left\{(s-1)\zeta_m(s)\right\},$$

nella quale il limite a destra s'intendeva per s reale positivo >1 e tendente a 1; però attualmente la (I^*) ci dimostra che la $\zeta_m(s)$ si comporta nell'intorno di $s=1$ come la $\zeta(s)$ ed ha ivi un polo del 1° ordine, il cui residuo per la (9) è precisamente gh. D'altra parte il residuo di $\zeta(s)$ abbiamo visto essere $=1$, onde segue dalla (I^*)

$$f(1) = gh$$

ed è quindi $f(1)$ certo diverso da zero (reale positivo). E siccome

$$f(1) = \mathcal{L}_{\omega}(1)\,\mathcal{L}_{\omega^2}(1)\ldots\mathcal{L}_{\omega^{m-2}}(1)$$

ne concludiamo che ciascuna delle serie:

$$(10)\qquad \mathcal{L}_{\alpha}(1) = \sum_n{}' \frac{\alpha^{\mathrm{ind}\,n}}{n}\qquad (\alpha \neq 1),$$

ha una somma <u>non nulla</u>. Questo risultato, a cui conducono così spontaneamente le ricerche sul numero delle classi nel corpo circolare, è di dimostrazione diretta assai difficile; esso è di fondamentale importanza per la celebre dimostrazione del teorema sulla progressione aritmetica data da Dirichlet, che accerta l'infinità dei numeri primi contenuti in una tale progressione, quan-

do il primo termine e la ragione sono numeri interi primi fra loro.

Ed ora la formola per il numero h delle classi nel corpo circolare $k(\varepsilon)$ si scriverà

$$h = \frac{1}{g} \prod_{\alpha} \mathcal{L}_{\alpha}(1),$$

e, per avere anche qui l'espressione di h sotto forma chiusa, conviene in primo luogo sommare la serie ( ), ciò che si fa con un procedimento affatto analogo a quello del § 56 per la serie $\sum \frac{(\mathfrak{D}, n)}{n}$ riducendone il calcolo a quello di un integrale definito di una funzione razionale. In secondo luogo, occorre calcolare il valore di g, e questo dipende (§ 50) dal regolatore delle unità nel corpo circolare. Le formole finali pel valore di h vennero date da Kummer sotto forma semplice, sulla quale qui non ci intratterremo maggiormente.

§ 59.

Preliminari pel prolungamento analitico della funzione $\zeta(s)$

Abbiamo più volte accennato che la funzione $\zeta(s)$ di Riemann, e quella generale $\zeta_K(s)$ di Dedekind, relativa ad un qualunque corpo algebrico, sono estendibili,

secondo i principii generali del prolungamento ana (Riemann-Wierstrass), a tutto il piano complesso, e riescono funzioni uniformi in tutto il piano con una sola singolarità polare del 1° ordine nel punto $s=1$, ove la prima $\zeta(s)$ ha residuo $=1$, e la generale $\zeta_K(s)$ un residuo, legato dalla formola di Dedekind (III) § 51 al numero h delle classi. Per la $\zeta(s)$, e per la zèta di Dedekind relative al corpo quadratico ed al corpo circolare, abbiamo inoltre già effettuato parzialmente il prolungamento analitico, dal semipiano $R(s)>1$ al semipiano $R(s)>0$.

Chiuderemo questi studi col dare, almeno per la $\zeta(s)$ di Riemann, il prolungamento analitico indicato a tutto il piano complesso, e fra le varie dimostrazioni che si hanno di questo fatto fondamentale ne sceglieremo una che lega la $\zeta(s)$ Riemanniana ad altre funzioni classiche dell'analisi, la Γ Euleriana, e le funzioni thèta ellittiche. La dimostrazione si fonda sopra una formola che appartiene alla teoria della trasformazione lineare delle funzioni ellittiche thèta ad una variabile, e verrà qui stabilita direttamente secondo un procedimento di Landesberg. Diciamo subi-

to che sulle formole corrispondenti per le funzioni θ a più variabili sono fondate le notevolissime e recenti ricerche di Hecke per la generale $\zeta_K(s)$ di Dedekind, dalle quali da ultimo daremo un cenno (§ 62).

Sia $\underline{x}$ una variabile, che supponiamo senz'altro (essendo sufficiente allo scopo nostro) reale e positiva, $x > 0$. Consideriamo la serie a termini positivi

$$(1) \qquad \sum_{n=-\infty}^{n=+\infty} e^{-n^2\pi x} = 1 + 2\sum_{1}^{\infty} e^{-n^2\pi x},$$

la cui convergenza è senz'altro manifesta, da che ponendo $q = e^{-\pi x}$, è $\underline{q}$ positiva e < 1, e la serie $1 + 2\sum_{1}^{\infty} q^{n^2}$ è convergente. Questa serie (1) (serie θ) rappresenta una funzione regolare della x, che indicheremo con

$$(1') \qquad \theta(x) = \sum_{-\infty}^{+\infty} e^{-n^2\pi x}.$$

Dimostreremo che essa soddisfa all'equazione funzionale

$$(I) \qquad \theta(x) = \frac{1}{\sqrt{x}}\, \theta\left(\frac{1}{x}\right),$$

dove per $\sqrt{x}$ intendiamo il valore positivo del radicale.

A tale scopo, usando un'analisi simile a quella di Kronecker al § 54 per il calcolo delle somme di Gauss, consideriamo la seguente funzione $f(s)$ della variabile complessa $\underline{s}$:

(2) $$f(s) = \frac{e^{-\pi x s^2}}{e^{2\pi i s} - 1} \quad ,$$

che è uniforme in tutto il piano e con sole singolarità polari del 1° ordine nei punti interi $s = n$ (n intero) dell'asse reale, col corrispondente residuo

(3) $$\frac{1}{2\pi i} \; e^{-n^2 \pi x} .$$

Separando in s la parte reale ed immaginaria, col porre $s = \sigma + it$, indichiamo con m un intero positivo, che faremo poi crescere infinitamente, e tracciamo nel piano s il rettangolo, simmetrico rispetto agli assi, compreso fra le due rette verticali

$$\sigma = m + \frac{1}{2} \quad , \qquad \sigma = -\left(m + \frac{1}{2}\right)$$

e le due orizzontali

$$t = 1 \quad , \qquad t = -1 .$$

Sul contorno L di questo rettangolo non vi sono poli della $f(s)$, data dalla (2), e nell'interno abbiamo i poli

$$s = 0 \, , \; \pm 1 \, , \; \pm 2 \, , \ldots \pm m .$$

Estendendo dunque l'Integrale $\int_L f(s)\, ds$ al contorno in verso positivo, pel valore $J(x)$ di questo integrale (che dipenderà da x), avremo pel teorema di Cauchy e per la (3):

$$(4) \qquad \mathcal{I}(x) = \int_{\mathfrak{L}} f(x)\,ds = \sum_{n=-m}^{n=m} e^{-n^2\pi x} .$$

Ora l'integrale $\mathcal{I}$ si spezza in quattro parti, le due $\mathcal{I}_1$, $\mathcal{I}_2$ estese ai tratti verticali del contorno, e le due $\mathcal{I}_3$, $\mathcal{I}_4$ estese a quelli orizzontali. Il secondo membro della (4), facendo crescere m infinitamente, converge verso la $\theta(x)$ data dalla (1'), e calcolando il limite del primo $\int_{\mathfrak{L}} f(x)\,ds$, troveremo che esso è precisamente $\frac{1}{\sqrt{x}}\,\theta\left(\frac{1}{x}\right)$, ciò che dimostrerà la formola (I).

a) Cominciamo dal far vedere che le due prime parti $\mathcal{I}_1$, $\mathcal{I}_2$ dell'integrale $\mathcal{I}(x)$ convergono ambedue a zero, al crescere infinito di $\underline{m}$. L'integrale $\mathcal{I}_1$ sia p.e. quello esteso al tratto

$$\mathcal{I}_1) \qquad s = \left(m + \tfrac{1}{2}\right) + it \qquad -1 \leq t < +1$$

e $\mathcal{I}_2$ quello esteso al tratto

$$\mathcal{I}_2) \qquad s = -\left(m + \tfrac{1}{2}\right) + it \qquad -1 \leq t \leq +1 .$$

Il modulo di $f(s)$ su questi tratti, ove $\sigma = \pm\left(m + \frac{1}{2}\right)$ è dato da

$$|f(s)| = \frac{e^{-\pi x\left(m+\frac{1}{2}\right)^2 + \pi x t^2}}{1 + e^{-2\pi t}} ,$$

ed essendo $|t| < 1$, si ha

$$|f(s)| < e^{-\pi x\left(m+\frac{1}{2}\right)^2 + \pi x}$$

valore che, indipendentemente da t, converge a zero

quando m cresce infinitamente. Su questi due tratti verticali, ciascuno dei quali ha lunghezza finita $= 2$, il modulo della $f(s)$ è dunque piccolo a piacere, per ciò anche quello dell'integrale; dunque

$$\lim_{m=\infty} J(x) = \lim_{m=\infty} (J_3 + J_4).$$

b) Per il calcolo del limite, per $m = \infty$, della somma $J_3 + J_4$ dei due integrali estesi ai tratti orizzontali, conviene ricordare che l'integrale fra limiti infiniti $\int_{-\infty}^{+\infty} e^{-\xi^2} d\xi$ ha valore finito, precisamente

$$\int_{-\infty}^{+\infty} e^{-\xi^2} d\xi = \sqrt{\pi}.$$

I due integrali estesi ai tratti orizzontali $t = \pm 1$ conservano ciascuno un senso anche estesi da $\sigma = -\infty$ a $\sigma = +\infty$, perchè quando $s = \sigma + i$ pel modulo dell'integrando $f(s)$ si ha

$$|f(s)| = \frac{e^{-\pi x \sigma^2 + \pi x}}{|e^{2\pi i s} - 1|} \leq \frac{e^{\pi x}}{1 - e^{-2\pi}} \cdot e^{-\pi x \sigma^2}$$

e, per quanto ora si è ricordato, questa espressione è integrabile rispetto a σ fra $-\infty$ e $+\infty$. Similmente pel secondo integrale, con $s = \sigma - i$, è

$$|f(s)| \leq \frac{e^{\pi x}}{e^{2\pi} - 1} \cdot e^{-\pi x \sigma^2}.$$

Indicando adunque con $\omega(x)$ la somma dei due integrali J_3, J_4 estesi fra limiti infiniti (col tener conto del

senso del percorso) abbiamo

$$(5)\qquad \omega(x)=\int_{-\infty-i}^{+\infty-i} f(s)\,ds-\int_{-\infty+i}^{+\infty+i} f(s)\,ds,\qquad f(s)=\frac{e^{-\pi x s^2}}{e^{2\pi i s}-1}.$$

e noi andiamo a calcolare separatamente i valori di questi due integrali, sviluppati opportunamente in serie.

D'altra parte, per quanto si è visto, è $\omega(x)=\lim_{m=\infty} \mathcal{T}(x)=\theta(x)$.

Per il primo integrale nella (5) essendo $s=\sigma-i$, è $\left|e^{2\pi i s}\right|=$ $=e^{2\pi}>1$ e la frazione $\frac{1}{e^{2\pi i s}-1}$ si può sviluppare nella serie $\sum_{n=-1}^{n=-\infty} e^{2n\pi i s}$, da cui

$$f(s)=\sum_{n=-1}^{n=-\infty} e^{-\pi x s^2+2n\pi i s}$$

e l'integrazione rispetto a σ tra $-\infty$ e $+\infty$ della serie si può fare eseguendola termine a termine sui termini della serie, perchè è integrabile fra $-\infty$ e $+\infty$ la serie dei moduli

$$e^{-\pi x(\sigma^2-1)}\sum_{n=-1}^{n=-\infty} e^{2n\pi}=\frac{e^{\pi x}}{e^{2\pi}-1}\cdot e^{-\pi x\sigma^2},$$

dunque si ha

$$\int_{-\infty-i}^{+\infty-i} f(s)\,ds=\sum_{n=-1}^{n=-\infty}\int_{-\infty-i}^{\infty-i} e^{-\pi x s^2+2n\pi i s}\,ds.$$

E pel secondo integrale nel quale $s=\sigma+i$, indi $\left|e^{2\pi i s}\right|=e^{-2\pi}<1$, si sviluppi similmente

$$\frac{1}{e^{2\pi i s}-1}=-\sum_{n=0}^{n=\infty} e^{2n\pi i s},$$

e si avrà con considerazioni analoghe

$$\int_{-\infty+i}^{\infty+i} f(s)\,ds = -\sum_{n=0}^{n=\infty} \int_{-\infty+i}^{\infty+i} e^{-\pi x s^2 + 2n\pi i s}\, ds.$$

Sostituendo nella (5) risulta

$$\omega(x) = \sum_{n=-1}^{n=-\infty} \int_{-\infty-i}^{\infty-i} e^{-\pi x s^2 + 2n\pi i s}\, ds + \sum_{n=0}^{n=\infty} \int_{-\infty+i}^{\infty+i} e^{-\pi x s^2 + 2n\pi i s}\, ds,$$

formola che si può scrivere

$$(6) \qquad \omega(x) = \sum_{n=-\infty}^{n=\infty} e^{-\frac{n^2\pi}{x}} \int_{-\infty \pm i}^{\infty \pm i} e^{-\pi x\left(s - \frac{ni}{x}\right)^2} ds,$$

dove ai limiti degli integrali va preso il segno inferiore per n negativo, il superiore per n positivo o nullo. Ma ora dimostriamo che nei termini della serie a destra nella (6) tutti gli integrali hanno un medesimo valore, più in generale l'integrale

$$\int e^{-\pi x z^2}\, dz \qquad (z = \xi + i\eta)$$

esteso a tutta una retta orizzontale $\eta = h$ del piano z da $\xi = -\infty$ a $\xi = +\infty$ ha un valore determinato e finito indipendente da h. Questo è immediato se indicando con h_1, h_2 due diverse ordinate si considera il rettangolo racchiuso dalle due orizzontali

$$\eta = h_1 \quad , \quad \eta = h_2$$

e dalle due verticali $\xi = \pm R$, ove si faccia poi crescere al

l'infinito k, e si applichino le considerazioni del principio del paragrafo alla trascendente intera $e^{-\pi x z^2}$. L'integrale esteso al contorno $\mathfrak{L}$ del rettangolo è zero pel teorema di Cauchy; ma i due estesi ai tratti verticali tendono a zero quando k cresce infinitamente e quindi i due estesi ai tratti orizzontali percorsi in verso concordante, mentre restano limitati quando k converge verso ∞, al limite (presi fra $-\infty$ e $+\infty$) risultano eguali.

Così il valor comune degli integrali a destra nella (6) è quello di

$$\int_{-\infty}^{+\infty} e^{-\pi x \xi^2} d\xi \;,$$

che col cangiamento di variabile $x\xi\sqrt{\pi} = y$ diventa $\frac{1}{\sqrt{\pi x}}\int_{-\infty}^{+\infty} e^{-y^2} dy = \frac{1}{\sqrt{x}}$. La formola (6) diventa per ciò

$$\omega(x) = \frac{1}{\sqrt{x}} \sum_{n=-\infty}^{n=+\infty} e^{-\frac{n^2\pi}{x}} \;,$$

cioè per la posizione (1')

$$\omega(x) = \frac{1}{\sqrt{x}}\, \theta\left(\frac{1}{x}\right).$$

Ma si è già notato sopra che $\omega(x) = \theta(x)$, onde risulta dimostrata la formola (I).

§ 60.

Prolungamento analitico della $\zeta(s)$ a tutto il piano. Equazione funzionale per la $\zeta(s)$.

Veniamo ora a porre in relazione la $\zeta(s)$ di Riemann colla $\Gamma(s)$ Euleriana.

Per maggior chiarezza consideriamo dapprima i valori reali positivi di s, e partiamo dalla definizione di $\Gamma(s)$ per integrale definito

$$\Gamma(s) = \int_0^\infty e^{-\xi} \xi^{s-1} d\xi,$$

che, mutando s in $\frac{s}{2}$ e ξ in $n^2\pi x$, con n intero positivo, scriviamo

$$\Gamma(\tfrac{s}{2}) = \int_0^\infty e^{-n^2\pi x} (n^2\pi x)^{\frac{s}{2}-1} \cdot n^2\pi\, dx,$$

ovvero

$$\pi^{-\frac{s}{2}} \Gamma(\tfrac{s}{2}) \frac{1}{n^s} = \int_0^\infty e^{-n^2\pi x} x^{\frac{s}{2}-1} dx.$$

Supposto ora $s>1$, diamo al numero n tutti i valori interi $1, 2, 3, \dots \infty$, e sommiamo le formole corrispondenti; la serie a sinistra converge ed ha per somma: $\pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s)$, onde converge quella a destra e si ha

$$\pi^{-\frac{s}{2}} \Gamma(\tfrac{s}{2}) \zeta(s) = \sum_{n=1}^{n=\infty} \int_0^\infty e^{-n^2\pi x} x^{\frac{s}{2}-1} dx.$$

Ma siccome tutti i termini sono positivi, è lecito invertire a destra i due segni di integrazione e di somma

(V.ᵢ Dini - Calcolo integrale, vol. II,), e scrivere

$$(7) \qquad \pi^{-\frac{s}{2}}\Gamma\left(\tfrac{s}{2}\right)\frac{1}{n^s} = \int_0^\infty x^{\frac{s}{2}-1}\left(\sum_{n=1}^{n=\infty} e^{-n^2\pi x}\right)dx = \int_0^\infty x^{\frac{s}{2}-1}\psi(x)\,dx,$$

dove si è posto

$$\psi(x) = \sum_{n=1}^{n=\infty} e^{-n^2\pi x}.$$

Per le formole del paragrafo precedente, questa $\psi(x)$ è legata alla $\theta(x)$ dalla relazione

$$\psi(x) = \frac{\theta(x)-1}{2},$$

e quindi, per la (I), soddisfa all'equazione funzionale

$$(8) \qquad \psi(x) = \frac{1}{\sqrt{x}}\,\psi\left(\frac{1}{x}\right) + \frac{1}{2\sqrt{x}} - \frac{1}{2}.$$

Decomponiamo nella (7) l'intervallo d'integrazione $(0,\infty)$ nei due $(0,1)$, $(1,\infty)$ e scriviamo

$$\pi^{-\frac{s}{2}}\Gamma\left(\tfrac{s}{2}\right)\frac{1}{n^s} = \int_0^1 x^{\frac{s}{2}-1}\psi(x)\,dx + \int_1^\infty x^{\frac{s}{2}-1}\psi(x)\,dx,$$

onde sostituendo nel primo integrale $\psi(x)$ il secondo membro della (8), avremo

$$\pi^{-\frac{s}{2}}\Gamma\left(\tfrac{s}{2}\right)\zeta(s) = \int_0^1 x^{\frac{s}{2}-\frac{3}{2}}\psi\left(\tfrac{1}{x}\right)dx + \int_1^\infty x^{\frac{s}{2}-1}\psi(x)\,dx +$$

$$+\frac{1}{2}\int_0^1 x^{\frac{s}{2}-\frac{3}{2}}dx - \frac{1}{2}\int_0^1 x^{\frac{s}{2}-1}dx.$$

I due ultimi integrali, essendo $s>1$, si eseguiscono subito e risulta

$$\frac{1}{2}\int_0^1 x^{\frac{s-3}{2}}dx - \frac{1}{2}\int_0^1 x^{\frac{s-2}{2}}dx = \frac{1}{s-1} - \frac{1}{s} = \frac{1}{s(s-1)},$$

e la precedente diventa

$$\pi^{-\frac{s}{2}}\Gamma\left(\tfrac{s}{2}\right)\zeta(s)-\frac{1}{s(s-1)}=\int_0^1 x^{\frac{s}{2}-\frac{3}{2}}\,\psi\left(\tfrac{1}{x}\right)dx+\int_1^\infty x^{\frac{s}{2}-1}\psi(x)\,dx.$$

Riconducendo il primo integrale ai limiti 1, ∞, col cangiarvi la variabile d'integrazione x in $\frac{1}{x}$, risulta

$$(9)\qquad \pi^{-\frac{s}{2}}\Gamma\left(\tfrac{s}{2}\right)\zeta(s)-\frac{1}{s(s-1)}=\int_1^\infty\left(x^{-\frac{s+1}{2}}+x^{\frac{s}{2}-1}\right)\psi(x)\,dx.$$

Dimostriamo ora che la funzione di $\underline{s}$ data dall'integrale nel secondo membro

$$(10)\qquad G(s)=\int_1^\infty\left(x^{-\frac{s+1}{2}}+x^{\frac{s}{2}-1}\right)\psi(x)\,dx$$

è una <u>trascendente</u> <u>intera</u> in $\underline{s}$. Intanto, se al limite superiore ∞ sostituiamo un limite finito $A>1$, comunque grande, è facile vedere che l'altra funzione di $\underline{s}$

$$\bar{G}(s)=\int_1^A\left(x^{-\frac{s+1}{2}}+x^{\frac{s}{2}-1}\right)\psi(x)\,dx$$

è una trascendente intera in $\underline{s}$. Per questo si osservi che la funzione integranda

$$\left(x^{-\frac{s+1}{2}}+x^{\frac{s}{2}-1}\right)\psi(x)=x^{-\frac{1}{2}}e^{-\frac{s}{2}\log x}\psi(x)+x^{-1}e^{\frac{s}{2}\log x}\psi(x)$$

essa stessa, una trascendente intera in $\underline{s}$, e nel suo è sviluppo per potenze di $\underline{s}$ il coefficiente di s^n è dato da

$$\frac{1}{n!}\left\{x^{-\frac{1}{2}}\left(-\tfrac{1}{2}\log x\right)^n\psi(x)+x^{-1}\left(\tfrac{1}{2}\log x\right)^n\psi(x)\right\},$$

e l'integrazione fra 1 e A, a causa della convergenza in egual grado della serie, si può eseguire termine a termine, onde il coefficiente di s^n nello sviluppo

di $G(s)$ sarà

$$\beta_n = \frac{1}{n!}\int_1^A \left\{ x^{-\frac{1}{2}}\left(-\tfrac{1}{2}\log x\right)^n \psi(x) + x^{-1}\left(\tfrac{1}{2}\log x\right)^n \psi(x) \right\} dx.$$

Se indichiamo con K un limite superiore per $\psi(x)$ nel tratto $(1, A)$ e consideriamo che ivi $x > 1$ e $\log x$ raggiunge il massimo $\log A$, ne deduciamo per β_n la limitazione

$$\beta_n < \frac{2AK(\log A)^n}{n!}.$$

La serie $\sum \beta_n s^n$ per $\bar{G}(s)$ è dunque minorante rispetto all'altra

$$2K \sum \frac{A(\log A)^n}{n!} \cdot s^n,$$

che è sempre convergente. Di qui segue che la $\bar{G}(s)$ è una trascendente intera. Si consideri ora che, se manteniamo s in un qualunque campo finito del piano s, la $G(s)$ è il limite verso il quale converge uniformemente, al crescere all'infinito di A, la $\bar{G}(s)$. E infatti in un tale campo il modulo di $x^{-\frac{s+1}{2}} + x^{\frac{s}{2}-1}$, variando x da 1 a ∞, rimane minore di

$$x^{-\frac{\sigma}{2}} + x^{\frac{\sigma}{2}} \qquad (\sigma = \mathcal{R}(s)),$$

cioè di $2x^a$ con a costante, ed ha già un significato ed è convergente

$$2\int_1^\infty x^a \psi(x)\, dx,$$

perchè, avendosi

$$\psi(x) = \sum_1^\infty e^{-n^2\pi x} < \sum_1^\infty e^{-n\pi x} < \frac{1}{e^{\pi x}-1},$$

è già convergente l'integrale maggiorante:

$$2\int_1^\infty \frac{x^a}{e^{\pi x}-1}\,dx.$$

La $G(s)$, come limite verso cui converge uniformemente la trascendente intera $\bar{G}(s)$ al crescere di A all'infinito, è essa stessa una trascendente intera, ciò che riconosciamo più da vicino riconducendo la questione ad una proprietà fondamentale ben nota, nel modo seguente. Diamo ad A la serie infinita di valori

$$A = 2, 3, \dots m+1, \dots$$

e chiamiamo

$$G_1(s),\ G_2(s) \cdots G_m(s) \cdots$$

le trascendenti intere $\bar{G}(s)$ corrispondenti. Allora $G_m(s)$, al crescere di m, converge uniformemente verso $G(s)$, cioè la serie

$$G_1(s) + \big(G_2(s) - G_1(s)\big) + \big(G_3(s) - G(s)\big) + \cdots + \big(G_m(s) - G_{m-1}(s)\big) + \cdots$$

è uniformemente convergente nel campo finito in considerazione, e la sua somma è $G(s)$. Dunque $G(s)$ è funzione della variabile complessa s, sempre fini-

ta, continua e monodroma in qualunque campo finito, vale a dire è una trascendente intera.

Così abbiamo stabilita la formola

$$(11) \qquad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{1}{s(s-1)} + \mathcal{G}(s),$$

dove la $\mathcal{G}(s)$ è una <u>trascendente</u> <u>intera</u>, e con questa formola manifestamente il prolungamento analitico della $\zeta(s)$ Riemanniana a tutto il piano complesso è effettuato.

Osserviamo ora che la $\mathcal{G}(s)$ data dalla (10), resta manifestamente invariata se si cangia l'argomento s in $1-s$, e lo stesso è della funzione $s(s-1)$, onde segue dalla (11) che della medesima proprietà gode il primo membro della (11). Siamo così giunti all'importante teorema (Riemann):

<u>La funzione</u> $\zeta(s)$ <u>Riemanniana soddisfa all'equazione funzionale</u>

$$(\mathrm{II}) \qquad \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{\frac{s-1}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Segue di qui che, coll'intermediario della Γ Euleriana, il calcolo di $\zeta(s)$ in un punto s del piano complesso si riduce a quello del valore della ζ nel punto $1-s$, e si osserverà che avendosi $\frac{1}{2}\left\{s+(1-s)\right\} = \frac{1}{2}$ questi due

punti sono <u>simmetrici</u> rispetto al punto di ascissa $\frac{1}{2}$ sull'asse reale. Basta quindi conoscere i valori che prende $\zeta(s)$ nel semipiano $\mathcal{R}(s) > \frac{1}{2}$ (a destra della retta $\sigma = \frac{1}{2}$) per conoscere anche quelli nel semipiano $\mathcal{R}(s) < \frac{1}{2}$ a sinistra.

§ 61

Conseguenze. - Zeri secondari e zeri principali della $\zeta(s)$.

Dalla formola (11), ricordando le ben note proprietà della Γ Euleriana:

a) L'inversa $\frac{1}{\Gamma(s)}$ della $\Gamma(s)$ è una trascendente intera (emiseno)

b) Gli infinitesimi di questa sono del 1° ordine e situati nei punti interi, non positivi, dell'asse reale: $s = 0, -1, -2 \ldots -m, \ldots$

si deducono facilmente per la $\zeta(s)$ di Riemann le proprietà seguenti:

1° <u>La funzione</u> $(s-1)\zeta(s)$ <u>è una trascendente intera.</u>

Difatti

$$(s-1)\zeta(s) = \frac{\pi^{\frac{s}{2}}}{s\Gamma(\frac{s}{2})} + \frac{\pi^{\frac{s}{2}}\varphi(s)}{\Gamma(\frac{s}{2})},$$

e qui il secondo termine è una trascendente intera;

ma tale è anche il primo perchè $\frac{1}{s\Gamma\left(\frac{s}{2}\right)}$ si serba finita anche per $s=0$.

2º <u>La funzione</u> $\zeta(s)-\frac{1}{s-1}$ <u>è una trascendente intera</u> $G_2(s)$. –

Difatti $(s-1)\zeta(s)=G_1(s)$ è una trascendente intera, che per $s=1$ prende il valore $G_1(1)=1$, indi nella decomposizione

$$\frac{G_1(s)}{s-1}=\frac{1}{s-1}+\frac{G_1(s)-1}{s-1},$$

il secondo termine è una trascendente intera $G_2(s)$.

In conclusione adunque:

3º <u>La funzione</u> $\zeta(s)$ <u>è regolare in tutto il piano complesso, coll'unica singolarità polare del 1º ordine in</u> $s=1$, <u>dove ha residuo</u> $=1$.

Per le leggi di frequenza dei numeri primi ha singolare importanza, come Riemann ha riconosciuto, la distribuzione degli <u>zeri</u> di $\zeta(s)$ nel piano complesso e precisamente di quelli che fra breve diremo gli zeri <u>principali</u> di $\zeta(s)$ per distinguerli da quelli <u>secondarii</u>, dovuti ai poli della Γ Euleriana. È utile per la ricerca di questi ultimi presentare l'equazione funzionale (II) per la $\zeta(s)$ sotto

una seconda forma, che si ottiene ricorrendo alle note proprietà della Γ date dalle due relazioni seguenti

$$\begin{cases} \Gamma(s)\,\Gamma(1-s) = \dfrac{\pi}{\operatorname{sen}(\pi s)} \\ \Gamma(s)\,\Gamma(s+\frac{1}{2}) = 2\sqrt{\pi}\; 2^{-2s}\,\Gamma(2s). \end{cases}$$

Cangiando in queste s in $\frac{1+s}{2}$ e dividendo, si ottiene

$$\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})} = \frac{2^{1-s}}{\sqrt{2\pi}} \cos\left(\frac{\pi s}{2}\right)\Gamma(s),$$

dopo di che la (II) si può scrivere sotto la seconda forma richiesta

$$(II^*) \qquad \zeta(1-s) = \frac{2}{(2\pi)^s} \cos\left(\frac{\pi s}{2}\right)\Gamma(s)\,\zeta(s).$$

Da questa, ovvero dalla (II), possiamo dedurre diverse conseguenze, ricordando dal § 45 che la $\zeta(s)$ non si annulla mai nel semipiano $R(s) > 1$. E allora dalla (II) risulta che nel semipiano $R(s) < 0$ il secondo membro della (II) non si annulla mai (perchè la $\Gamma(s)$ non ha zeri), e non può quindi annullarsi in $R(s) < 0$ nemmeno il primo membro. Ma la $\Gamma(\frac{s}{2})$ diventa ivi infinita in tutti e soli i punti

$$(12) \qquad s = -2, -4, \dots -2m, \dots$$

e per ciò la $\zeta(s)$, in questo semipiano $R(s) < 0$, ha in questi punti ed in questi soltanto zeri del 1° ordine.

Dunque intanto: <u>all'esterno della striscia fra le due verticali $\mathcal{R}(s)=0$, $\mathcal{R}(s)=1$ non esistono altri zeri della $\zeta(s)$ che nei punti (12) dell'asse reale negativo.</u>

Ma è facile vedere che nemmeno nel tratto (0,1) dell'asse reale, estremi inclusi, esistono altri zeri della $\zeta(s)$. Quanto agli estremi, nell'estremo $s=1$ la $\zeta(s)$ diventa invece infinita, e in $s=0$, ove la $\Gamma(s)$ diventa infinita del 1° ordine, non può annullarsi la $\zeta(s)$, perchè allora il secondo membro della (II*) resterebbe finito per $s=0$, mentre al contrario il primo diventa infinito. Quando poi s è reale $=\sigma$, ed interno al tratto (0,1), la formola (IV) del § 46

$$\zeta(\sigma)=\frac{1}{1-2^{1-\sigma}}\left\{1-\frac{1}{2^\sigma}+\frac{1}{3^\sigma}-\frac{1}{4^\sigma}+\cdots\right\}$$

dimostra che per $0<\sigma<1$, il primo fattore $\frac{1}{1-2^{1-\sigma}}$ è negativo e invece il secondo dato dalla somma della serie $1-\frac{1}{2^\sigma}+\frac{1}{3^\sigma}-\cdots$ è positivo, per ciò si ha costantemente

$$\zeta(\sigma)<0\,,\quad \text{quando}\quad 0<\sigma<1\,;$$

dunque: <u>in tutto il tratto (0,1) non vi sono zeri della $\zeta(s)$.</u>

Risulta da queste considerazioni che sull'asse reale la $\zeta(s)$ non presenta che gli zeri secondari della serie

(12), e tutti gli altri zeri della $\zeta(s)$ (ove esistano) sono quindi immaginarii e situati nella striscia compresa fra le due parallele $\sigma = 0$, $\sigma = 1$. Ma si può dimostrare di più che sulle due rette stesse, contorno della striscia, non esistono zeri di $\zeta(s)$. Basta dimostrare questo per una delle parallele p.e. per la $\sigma = 1$, perchè se vi fosse uno zero sull'asse immaginario $\sigma = 0$ in $s = 1 - it$ ($t \neq 0$), a causa dell'equazione funzionale (II), se ne avrebbe un altro in $s = 1 - it$ sulla retta $\sigma = 1$. Dimostriamo adunque:

La $\zeta(s)$ non può essere nulla per $s = 1 + it$ $(t \neq 0)$.

Per questo ricordiamo che per $\sigma = \Re(s) > 1$ valgono per la $\zeta(s)$ gli sviluppi in serie e prodotto infinito (III), (III*) del § 45 e conseguentemente anche pel suo logaritmo la formula d'Eulero (II) § 44 (nella quale è da porsi $f(n) = \frac{1}{n^s}$)

$$\log \zeta(s) = \sum_p \sum_m \frac{1}{m p^{ms}} \qquad (\Re(s) > 1),$$

dove la serie doppia (nella quale p percorre i numeri primi e m tutti gli interi) ha convergenza assoluta ed uniforme. È lecita quindi la derivazione per serie e ne risulta

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p \sum_m \frac{\log p}{p^{ms}} \qquad (\mathcal{R}(s) > 1),$$

Supposto sempre $\sigma > 1$ poniamo in questa successivamente $s = \sigma$, $\sigma + it$, $\sigma + 2it$ e prendendo le parti reali avremo

$$\frac{\zeta'(\sigma)}{\zeta(\sigma)} = -\sum_p \sum_m \frac{\log p}{p^{m\sigma}}$$

$$\mathcal{R}\left[\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)}\right] = -\sum_p \sum_m \frac{\log p \cos(mt \log p)}{p^{m\sigma}}$$

$$\mathcal{R}\left[\frac{\zeta'(\sigma+2it)}{\zeta(\sigma+2it)}\right] = -\sum_p \sum_m \frac{\log p \cos(2mt \log p)}{p^{m\sigma}}$$

Moltiplicando la prima per 3, la seconda per 4, e sommando colla terza risulta

$$(13) \qquad 3\,\frac{\zeta'(\sigma)}{\zeta(\sigma)} + 4\,\mathcal{R}\left[\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)}\right] + \mathcal{R}\left[\frac{\zeta'(\sigma+2it)}{\zeta(\sigma+2it)}\right] =$$

$$= -\sum_p \sum_m \frac{\log p \cdot \{3 + 4\cos(mt \log p) + \cos(2mt \log p)\}}{p^{m\sigma}}$$

Ma per qualunque angolo φ è sempre

$$3 + 4\cos\varphi + \cos 2\varphi = 2(1 + \cos\varphi)^2 \geq 0$$

e per ciò nella (13) tutti i termini a destra hanno lo stesso segno e il valore del secondo membro è negativo o nullo. Siamo così pervenuti alla diseguaglianza (valida per σ reale > 1 e per qualunque t)

$$(14) \qquad 3\,\frac{\zeta'(\sigma)}{\zeta(\sigma)} + 4\,\mathcal{R}\left[\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)}\right] + \mathcal{R}\left[\frac{\zeta'(\sigma+2it)}{\zeta(\sigma+2it)}\right] \leq 0,$$

e di qui possiamo facilmente dedurre che non può esₑ sere $\zeta(1+it)=0$ $(t \neq 0)$. Supponiamo al contrario che in $s=1+it$ vi sia uno zero di $\zeta(s)$, diciamo d'ordine $k>0$, ed in $s=1+2it$, eventualmente, uno zero d'ordiₑ ne $l \geq 0$, talchè la derivata logaritmica $\frac{\zeta'(s)}{\zeta(s)}$ avrà in $s=1+it$ un polo del 1° ordine di residuo k e in $s=1+2it$ (eventualmente) un polo del 1° ordine di resiₑ duo $\underline{l}$, mentre in $s=1$ (dove $\zeta(s)$ ha polo del 1° ordine) la $\frac{\zeta'(s)}{\zeta(s)}$ ha un polo di residuo $\underline{-1}$. Se moltiplichiamo la diseguaglianza (14) per $\sigma-1$ $(\sigma>1)$ e passiamo al liₑ mite per σ convergente a $\underline{1}$ dalla destra, ne deduciaₑ mo

$$-3+4k+l \leq 0$$

e perciò

$$k \leq \frac{3-l}{4} \leq \frac{3}{4},$$

Da tutto ciò si raccoglie: <u>Gli zeri principali della $\zeta(s)$ Riemanniana sono tutti situati internamenₑ te alla striscia del piano complesso compresa fra le due parallele $\Re(s)=0$, $\Re(s)=1$ e sono tutti immagiₑ narii.</u>

Che esistano in effetto infiniti zeri principali per la

$\zeta(s)$ venne asserito da Riemann, insieme ad altre proprietà concernenti la loro distribuzione, e le relazioni colla frequenza dei numeri primi. La maggior parte delle asserzioni di Riemann vennero poi dimostrate da successive ricerche di altri autori (Hadamard - De la Vallée Poussin, ecc.); ma fra queste la proposizione: Tutti gli zeri principali della $\zeta(s)$ hanno la parte reale $= \frac{1}{2}$ (cadono sulla retta media della striscia) non ha ancora ricevuto una dimostrazione e rimane dubbia.

§ 62

Cenno sulle ricerche di Hecke per l'estensione dei risultati alla $\zeta_K(s)$ di Dedekind.

Come più volte abbiamo accennato, le proprietà della $\zeta(s)$ Riemanniana, quale funzione regolare della variabile complessa s in tutto il piano complesso, salvo nel polo del primo ordine $s = 1$, sono state estese recentemente nelle importanti ricerche di Hecke alla funzione $\zeta_K(s)$ di Dedekind per qualunque corpo algebrico.

Pur rinunciando qui alla esposizione di queste notevoli

lissime ricerche diremo che, in analogia colla formola (I) § 59 pel caso del corpo razionale, esse si fondano sulle formole di trasformazione lineare delle funzioni θ a più variabili, e ci limiteremo a dare gli enunciati delle proposizioni fondamentali stabilite da Hecke. Nel recente libro di Landau: Einführung in die elementare und analytische Theorie der algebraischen Zahlen und Ideale (Leipzig-Teubner, 1918), il lettore troverà sviluppata questa nuova teoria, insieme alle ulteriori conseguenze sulla distribuzione degli zeri della $\zeta_K(s)$, strettamente collegata alla frequenza degli ideali primi nel corpo algebrico.

Nei seguenti enunciati delle prime proposizioni di Hecke, per evitare equivoci con notazioni già usate nelle presenti lezioni, la variabile complessa, argomento della ζ_K anzichè con s, sarà denotata coll'ordinario simbolo z; e le lettere r, s indicheranno, come prima, la prima r il numero dei corpi reali fra i coniugati del corpo fondamentale K, la seconda s il numero delle coppie dei corpi complessi coniugati. Ancora sarà posto $\nu = r+s$, talchè sarà $\nu-1$ il numero del

le unità indipendenti nel corpo.

Ciò premesso, ecco come si enunciano le accennate proposizioni fondamentali di Hecke:

A) La funzione $\zeta_K(z)$ di Dedekind, relativa a qualunque corpo algebrico, è prolungabile analiticamente a tutto il piano complesso z, ed è ivi uniforme e dappertutto regolare, salvo in $z=1$, dove presenta una singolarità polare del 1° ordine col residuo gh di Dedekind (§ 51).

I punti di infinitesimo della $\zeta_K(z)$ sono di due specie, che distinguiamo ancora in secondarii, dipendenti dai poli della Γ Euleriana, ed in principali.

Per i primi sussistono le proprietà seguenti:

B) Gli zeri secondarii di $\zeta_K(z)$ sono tutti situati sull'asse reale negativo in punti interi (di affissa intera), così enumerati: α) in $z=0$ uno zero d'ordine d'ordine $\nu-1$, infinitesimo che sparisce quando $\nu=1$ (corpo razionale o corpo quadratico immaginario); β) nei punti interi negativi pari $z=-2k$ zeri d'ordine ν; γ) nei punti interi negativi impari $z=-(2k+1)$ zeri di ordine s eguale al numero delle coppie dei corpi immaginarii [infinitesimi che spariscono se gli n cor-

pi coniugati sono tutti reali].

Per gli zeri di seconda specie si ha:

C) <u>Esistono infiniti zeri principali della</u> $\zeta_K(z)$, <u>tutti immaginarii e collocati internamente alla striscia fra le due parallele</u> $\mathcal{R}(z)=0$, $\mathcal{R}(z)=1$.

In fine come per la $\zeta(z)$, così per la $\zeta_K(z)$, sussiste una equazione funzionale che, nel caso generale, assume la forma seguente:

D) <u>Indicando con A la costante</u>

$$A = 2^{-s}\,\pi^{-\frac{n}{2}}\sqrt{|\mathfrak{D}|}$$ (n grado del corpo, $\mathfrak{D}$ numero fondamentale)

<u>la</u> $\zeta_K(z)$ <u>soddisfa all'equazione funzionale seguente</u>

$$A^z\left(\Gamma\left(\tfrac{z}{2}\right)\right)^r\left(\Gamma(z)\right)^s\zeta_K(z) = A^{1-z}\left(\Gamma\left(\tfrac{1-z}{2}\right)\right)^r\left(\Gamma(1-z)\right)^s\zeta_K(1-z).$$

Osserveremo che in questa equazione funzionale sono già contenuti i risultati segnalati in B) per la situazione degli zeri secondarii ed i loro ordini. E se da ultimo ritorniamo ancora sui risultati speciali, ottenuti rispettivamente ai §§ 52 e 58 per il prolungamento analitico della $\zeta_K(z)$ al semipiano $\mathcal{R}(z)>0$, nel caso del corpo quadratico e nell'altro del corpo circolare $k(\varepsilon)$, ricorderemo che ivi abbiamo trovato

a) $$\zeta_K(z) = \zeta(z)\cdot f(z),$$

dove

b) $$f(z) = \sum_n \frac{(D,n)}{n^z}, \quad \text{nel caso del corpo quadratico}$$

c) $$f(z) = \prod_\alpha \left(\sum_n \frac{\alpha^{\mathrm{ind}\,n}}{n^z}\right) \quad \alpha = \omega, \omega^2, \ldots \omega^{m-1} \left(\omega = e^{\frac{2\pi i}{n}}\right.$$

nel caso del corpo circolare),

ed in ambedue i casi si è visto che la $f(z)$ è regolare in tutto il semipiano $R(z) > 0$, e quindi in particolare nell'interno della striscia fra le due parallele $R(z) = 0$, $R(z) = 1$. Ma ora, osservando la formola (a), segue manifestamente, dalle proposizioni di Hecke, che tutti gli zeri della funzione $\zeta(z)$ di Riemann, tanto i secondarii (ciò che accade in generale) come i principali sono zeri, almeno dello stesso ordine, per la $\zeta_K(z)$ del corpo quadratico e del circolare. E poichè $\zeta_K(z)$ e $\zeta(z)$ hanno anche a comune l'unico polo $z=1$ del 1° ordine, si conclude che la funzione

$$f(z) = \frac{\zeta_K(z)}{\zeta(z)}$$

è priva affatto di singolarità nel piano complesso e quindi:

<u>Le funzioni definite dalle formole (b) e (c), rispettivamente nel caso dei corpi quadratici e nel caso del corpo circolare $k(\varepsilon)$, sono due trascendenti intere.</u>

NOTA I.

al § 7 pag: 48

Si è ivi asserito che il fenomeno dell'esistenza, in un corpo algebrico, di numeri α indecomponibili, e che tuttavia non funzionano come numeri primi, è indissolubilmente legato all'altro che esistono nel corpo ideali secondarii (non principali), o in altre parole:

A) In un corpo algebrico K esistono numeri α indecomponibili come numeri, e pur tuttavia decomponibili come ideali (α), allora ed allora soltanto che esistono ideali secondarii.

Indicando con h il numero delle classi degli ideali (§ 33), dobbiamo dunque provare che se $h=1$ tutti i numeri α indecomponibili funzionano anche come numeri primi, e se invece $h>1$ vi sono numeri α indecomponibili come numeri ed invece decomponibili come ideali (α).

a) Sia $h=1$, cioè tutti gli ideali siano principali. Se un numero α è indecomponibile come numero, è anche indecomponibile come ideale (α), perchè ove si ave-

se nel caso contrario $(\alpha)=(\beta)(\gamma)$ sarebbe anche $\alpha=\beta\gamma$.

b) Sia invece $h>1$ ed esistano quindi ideali A secondarii. Gli ideali fattori primi di A non potranno essere tutti principali, chè altrimenti sarebbe anche A principale. Sia dunque P un ideale primo secondario (non principale), e sia δ l'esponente >1 e divisore di h a cui P appartiene, cioè sia P^δ la minima potenza di P che dà luogo ad un ideale principale $P^\delta=(\alpha)$. Il numero α è decomponibile come ideale in δ fattori $=P$; ma come numero è indecomponibile perchè ove si avesse

$$\alpha=\beta\gamma \quad , \text{ indi } \quad (\beta)(\gamma)=P^\delta,$$

risulterebbe $(\beta)=P^r$, $(\gamma)=P^s$ con r, s interi positivi e $\delta=r+s$. In tal caso P^r con $0<r<\delta$ sarebbe già un ideale principale, ciò che contraddice all'ipotesi.

NOTA II.

Complementi ai teoremi di Minkowski (§ 16 pag. 101).

Il teorema II pag. 101 assicura che, date n forme lineari $f_1, f_2, \dots f_n$, a coefficienti reali e a determinante positivo $\mathfrak{D}$, e scelte n quantità positive $\mathfrak{D}_1, \mathfrak{D}_2, \dots \mathfrak{D}_n$ tali che $\mathfrak{D}_1 \mathfrak{D}_2 \dots \mathfrak{D}_n = \mathfrak{D}$, esistono valori interi, non tutti nulli, delle variabili $x_1, x_2, \dots x_n$, tali che i valori (non tutti nulli) assunti dalle n forme soddisfino alle diseguaglianze

$$|f_1| \leq \mathfrak{D}_1, \quad |f_2| \leq \mathfrak{D}_2, \quad \dots \quad |f_n| \leq \mathfrak{D}_n.$$

Partendo da questo risultato si può facilmente precisarlo vieppiù e dimostrare che: <u>si possono prendere per $x_1, x_2, \dots x_n$ degli interi non tutti nulli in modo che in $n-1$ delle diseguaglianze precedenti il segno di eguaglianza resti escluso, e si abbia per es.</u>

$$|f_1| < \mathfrak{D}_1, \quad |f_2| < \mathfrak{D}_2 \quad \dots \quad |f_{n-1}| < \mathfrak{D}_{n-1}, \quad |f_n| \leq \mathfrak{D}_n.$$

Per dimostrarlo si può usare il procedimento seguente (Hurwitz). Presa una quantità σ piccola a piacere, pongasi

$$\mathfrak{D}'_1 = \mathfrak{D}_1(1-\sigma), \quad \mathfrak{D}'_2 = \mathfrak{D}_2(1-\sigma), \dots \mathfrak{D}'_{n-1} = \mathfrak{D}_{n-1}(1-\sigma), \quad \mathfrak{D}'_n = \frac{\mathfrak{D}_n}{(1-\sigma)^{n-1}},$$

soddisfacendo così alla condizione

$$D'_1 D'_2 \ldots D'_n = D.$$

Pel citato teorema II pag. 101, potremo soddisfare le diseguaglianze

$$|f_1| \leq D_1(1-\sigma), \quad |f_2| \leq D_2(1-\sigma), \ldots |f_{n-1}| \leq D_{n-1}(1-\sigma), \quad |f_n| \leq \frac{D_n}{(1-\sigma)^{n-1}},$$

e questo comunque piccolo sia preso σ; e a più forte ragione saranno dunque soddisfatte le altre

$$(a) \quad |f_1| < D_1, \quad |f_2| < D_2, \ldots |f_{n-1}| < D_{n-1}, \quad |f_n| \leq \frac{D_n}{(1-\sigma)^{n-1}}.$$

Ora diamo a σ una serie infinita di valori positivi decrescenti

$$\sigma', \sigma'', \ldots \sigma^{(r)} \ldots$$

per modo che sia $\lim_{r=\infty} \sigma^{(r)} = 0$. Siccome le diseguaglianze (a) limitano superiormente i valori di $f_1, f_2, \ldots f_n$, ne risultano anche limitati i valori assoluti degli interi $x_1, x_2, \ldots x_n$ soddisfacenti alle diseguaglianze

$$(a') \quad |f_1| < D_1, \quad |f_2| < D_2, \ldots |f_{n-1}| < D_{n-1}, \quad |f_n| \leq \frac{D}{(1-\sigma^{(r)})^{n-1}},$$

e per ciò una stessa combinazione almeno di valori interi (non tutti nulli) per le $x_1, x_2 \ldots x_n$ dovrà presentarsi infinite volte, diciamo per $r = i_1, i_2, \ldots i_m, \ldots$ Se poniamo per semplicità $\sigma^{(i_1)} = \varepsilon_1$, $\sigma^{(i_2)} = \varepsilon_2, \ldots \sigma^{(i_m)} = \varepsilon_m, \ldots$ le ε_i stesse formano una serie infinita di quantità po-

sitive decrescenti, che tende al limite zero. E per un sistema di valori interi fissi di $x_1, x_2 \dots x_n$, diciamo $x_1 = p_1$, $x_2 = p_2$, $\dots$ $x_n = p_n$ sono sempre soddisfatte le diseguaglianze

$$|f_1| < D_1, \quad |f_2| < D_2, \; \dots |f_{n-1}| < D_{n-1} \quad |f_n| \leq \frac{D_n}{(1-\varepsilon_m)^{n-1}}$$

per tutti i valori dell'indice m. Ma siccome i primi membri rimangono fissi, ed è $\lim\limits_{m=\infty} \varepsilon_m = 0$, se ne conclude, passando al limite per $m = \infty$, che il medesimo sistema dei valori $(p_1, p_2, \dots p_n)$ per $x_1, x_2, \dots x_n$ soddisfa anche alle diseguaglianze

$$|f_1| < D_1, \quad |f_2| < D_2, \; \dots |f_{n-1}| < D_{n-1}, \; |f_n| \leq D_n, \quad \text{c.d.d.}$$

Dimostrato così il teorema II) nel nuovo modo più preciso, è chiaro come è da precisare analogamente il teorema III) pag. 104, relativo al caso in cui r delle forme siano reali e le rimanenti $n - r = 2s$ a coppie coniugate immaginarie.

NOTA III.

Cenno sul significato geometrico dei teoremi di Minkowski.

Si è già accennato, a pag. 90, che da considerazioni geometriche venne condotto il Minkowski alla scoperta dei suoi teoremi fondamentali sulle forme lineari; ma in questa nota aggiungiamo che questi teoremi sono alla loro volta casi particolarissimi di notevoli teoremi generali del Minkowski stesso sui corpi convessi (o meglio non concavi), teoremi che consentono importanti applicazioni geometriche ed aritmetiche (V. i due libri del Minkowski citati a pag. 90). Volendo qui dare un' idea del teorema fondamentale sui corpi convessi, cominciamo dall' interpretare geometricamente il teorema II) § 16. E sebbene le considerazioni siano generali, per qualunque numero n di variabili, limitiamoci al caso $n = 3$, ove potremo usare la figurazione nello spazio ordinario, laddove, per n qualunque, è da usarsi l'interpretazione analoga negli iperspazii.

Indichiamo con x, y, z le tre variabili, ed interpre-

tiamole come coordinate cartesiane nello spazio, che prenderemo per semplicità ortogonali, sebbene non faccia differenza alcuna il supporle invece oblique (ed anche il supporre diversa l'unità di misura secondo i tre assi).

Consideriamo l'insieme dei punti dello spazio aventi coordinate intere (m_1, m_2, m_3) e questo diciamo reticolo, mentre daremo il nome di vertici o nodi del reticolo ai punti stessi. Prendasi ora un cubo, col centro nel nodo origine $(0, 0, 0)$, colle facce parallele ai piani coordinati, e racchiuso quindi dalle tre coppie di piani paralleli

$$x = \pm h, \quad y = \pm h, \quad z = \pm h,$$

dove h è una costante positiva. È chiaro che se $h < 1$ (se il volume V del cubo è < 8) nessun altro nodo, oltre l'origine, si trova nel cubo, nè internamente, nè in superficie; ma appena $h \geq 1$ (quando $V \geq 8$) entrano nel cubo coppie di nodi opposti o internamente (per $V > 8$), o in superficie $(V = 8)$.

Ciò premesso, cominciamo dal dimostrare che al citato teorema II) (pag. 101) si può dare la forma geometrica

seguente:

<u>Se un qualunque parallelepipedo avente il centro nell'origine, e comunque orientato, ha un volume $V \geq 8$, esso contiene certamente o all'interno o in superficie, qualche coppia di nodi opposti del reticolo (oltre il centro).</u>

Scriviamo infatti le equazioni delle tre coppie di piani paralleli e simmetrici rispetto all'origine (centro), costituenti le facce, sotto la forma:

$$(1) \qquad \begin{cases} a_{11}x + a_{12}y + a_{13}z = \pm k_1 \\ a_{21}x + a_{22}y + a_{23}z = \pm k_2 \\ a_{31}x + a_{32}y + a_{33}z = \pm k_3 \end{cases}$$

dove k_1, k_2, k_3 denotano tre costanti positive e il determinante $D = |\alpha_{ik}|$ delle tre forme lineari dei primi membri delle (1),

$$\xi = a_{11}x + a_{12}y + a_{13}z \ , \ \eta = a_{21}x + a_{22}y + a_{23}z, \ \zeta = a_{31}x + a_{32}y + a_{33}z,$$

<u>che è certo diverso da zero</u>, si potrà supporre senz'altro $= 1$. Il volume V di questo parallelepipedo, cioè il valore dell'integrale triplo $\iiint dx\,dy\,dz$, esteso al campo $-k_1 < \xi < k_1$, $-k_2 < \eta < k_2$, $-k_3 < \zeta < k_3$, si calcola subito osservando che, dall'essere $\frac{\partial(\xi, \eta, \zeta)}{\partial(x, y, z)} = D = 1$, segue

$$V = \int_{-k_1}^{k_1} d\xi \int_{-k_2}^{k_2} d\eta \int_{-k_3}^{k_3} d\zeta = 8\, k_1 k_2 k_3 .$$

Ora se supponiamo $k_1 k_2 k_3 = 1$, coll'applicare il detto teorema II) (pág. 101) facendo $\mathfrak{D}_1 = k_1$, $\mathfrak{D}_2 = k_2$, $\mathfrak{D}_3 = k_3$, vediamo che, quando V raggiunge il valore 8, esiste almeno una coppia di valori <u>interi</u> opposti per x, y, z (non tutti nulli (pei quali)

$$|\xi| \leq k_1 , \quad |\eta| \leq k_2 , \quad |\zeta| \leq k_3$$

e il parallelepipedo contiene almeno una coppia di nodi opposti, secondo l'enunciato del teorema. Ed ora chiaramente se il parallelepipedo ha volume > 8, si avrà almeno una tale coppia nell'interno.

I parallelepipedi sopra considerati sono casi particolari di corpi <u>convessi</u>, o almeno non concavi, dotati di un centro in un nodo della rete e il teorema è un caso particolare del seguente:

A) <u>Se un corpo convesso (non concavo), e dotato di centro in un nodo del reticolo, ha un volume $V \geq 8$, esso contiene, oltre il centro, qualche altra coppia di nodi opposti del reticolo o all'interno o in superficie.</u> -

Rimandando per la dimostrazione rigorosa alle pagine 60 e seguenti delle Diophantische Approximatio-

neu di Minkowski, qui ci limitiamo ad esporre le considerazioni geometriche seguenti che lo giustificano.

Pensiamo un qualunque corpo convesso C avente centro nell'origine O, e di dimensioni così piccole da escludere (lasciare all'esterno) ogni altro nodo della rete; sia Ω il suo volume attuale. Assoggettiamo il corpo C ad una omotetia continua rispetto ad O, dilatandolo nel rapporto $t > 1$, dopo di che il volume diventerà $t^3\Omega$. Se facciamo crescere t dal valore iniziale $t = 1$, vi sarà un primo valore di t, diciamo $t = M$, pel quale il corpo dilatato viene a contenere una coppia (almeno) di nodi opposti in superficie, e questo corpo dilatato diciamo corpo (M). Riduciamo il corpo (M) alle dimensioni metà, cioè consideriamo il corpo corrispondente a $t = \frac{M}{2}$, che diciamo il corpo $\left(\frac{M}{2}\right)$; ed ora circondiamo ogni altro nodo, come centro, di un corpo eguale a questo $\left(\frac{M}{2}\right)$, trasportandovelo colla traslazione che porta l'origine O nel nuovo centro. Appunto perchè il corpo (M) è convesso, e solo in superficie contiene coppie di nodi opposti, si vede geometricamente (Minkowski l. c.) che uno qualunque di questi

corpi $\left(\frac{M}{2}\right)$ non è mai compenetrato da nessun altro e soltanto con corpi $\left(\frac{M}{2}\right)$ contigui ha a comune punti in superficie o tratti superficiali. Il loro insieme non riempie dunque generalmente nemmeno tutto lo spazio, nel quale rimarranno lacune periodiche. Ma invece se prendiamo il cubo $x = \pm\frac{1}{2}$, $y = \pm\frac{1}{2}$, $z = \pm\frac{1}{2}$ di volume $= 1$, la sua ripetizione periodica riempie una ed una sola volta tutto lo spazio senza lacune, onde si inferisce che il volume del corpo $\left(\frac{M}{2}\right)$ non supera 1, cioè $\left(\frac{M}{2}\right)^3\Omega \leq 1$, e perciò il volume del corpo (M) non supera 8: $M^3\Omega \leq 8$. Dunque se un corpo convesso col centro in O, simile al corpo iniziale $(t=1)$ di volume Ω, ha volume $V > 8$, per esso è certo $t > M$, onde contiene nel suo interno (oltre O) almeno due nodi opposti del reticolo. Quando poi sia $V = 8$, allora è $t = M$ e il corpo conterrà almeno una coppia di nodi opposti in superficie, come è asserito nel teorema A).

NOTA IV.

Sulle unità ridotte.

Nel teorema finale di Dirichlet sulla composizione delle unità (pag. 139) si è visto che le unità ridotte sono tutte e sole le radici dell'unità contenute nel corpo $K(\theta)$. I moduli di una tale unità, e di tutte le loro associate, sono eguali a 1, e tale proprietà, come facilmente vediamo, è caratteristica per queste unità ridotte cioè: <u>ogni intero ρ in $K(\theta)$ che abbia modulo $= 1$, insieme a tutti i suoi associati, è un'unità ridotta.</u>
Che sia un'unità è manifesto perchè la sua norma $N(\rho) = \rho\rho'\rho''\dots\rho^{(n-1)}$ è un intero razionale di valore assoluto $= 1$, e per ciò $N(\rho) = \pm 1$; ma di più se l'esprimiamo, col teorema di Dirichlet, per un sistema fondamentale di unità, tutti i suoi logaritmi associati sono nulli, cioè i suoi esponenti sono nulli, ed è quindi un'unità ridotta.

La stessa cosa si può provare, senza ricorrere al teorema di Dirichlet, colle considerazioni seguenti dovute a Minkowski (Geometrie der Zahlen §43) le quali ser-

vono, di più, ad assegnare un limite superiore pel numero delle unità ridotte.

Sia η un intero del corpo $K(\theta)$ dotato della proprietà che il suo modulo sia $=1$, insieme a quelli di tutti gli associati, ed essendo $[\omega_1, \omega_2, \dots \omega_n]$ una base del corpo, abbiasi

$$\eta = p_1\omega_1 + p_2\omega_2 + \dots + p_n\omega_n ,$$

in generale

$$\eta^{(r)} = p_1\omega_1^{(r)} + p_2\omega_2^{(r)} + \dots + p_n\omega_n^{(r)} ,$$

con $p_1, p_2, \dots p_n$ numeri razionali interi, che saranno inoltre primi fra loro, poichè se avessero un comune divisore q, sarebbe $\frac{\eta}{q}$ un intero con $\left|N\left(\frac{\eta}{q}\right)\right| = \frac{1}{q^n}$, il che è assurdo. Sia ora

$$\zeta = q_1\omega_1 + q_2\omega_2 + \dots + q_n\omega_n$$

un altro intero di $K(\theta)$ colle stesse proprietà: $|\zeta^{(r)}| = 1$; dico che: <u>se sussistono le congruenze simultanee</u>

$$p_1 \equiv q_1 \ , \ p_2 \equiv q_2 \cdots p_n \equiv q_n \qquad (\text{mod } 2)$$

<u>è necessariamente $\zeta = -\eta$ $(q_i = -p_i)$</u>. In caso contrario per l'intero $\frac{\eta - \zeta}{2}$, e per i coniugati, avremmo

$$\left|\frac{\eta^{(r)} - \zeta^{(r)}}{2}\right| \leq \frac{1}{2}\left\{|\eta^{(r)}| + |\zeta^{(r)}|\right\} \leq 1 ;$$

ma siccome $|\eta^{(r)}| = |\xi^{(r)}| = 1$, e non è $\xi = \pm \eta$, il segno d'eguaglianza resta escluso, onde

$$\left| \frac{\eta^{(r)} - \xi^{(r)}}{2} \right| < 1.$$

Per la norma dell'intero non nullo $\frac{\eta - \xi}{2}$ si avrebbe dunque $\left| N\left(\frac{\eta-\xi}{2}\right) \right| < 1$, ciò che è assurdo. Risulta di qui che, al massimo, il numero di questi numeri η potrà eguagliare il doppio del numero delle disposizioni distinte (mod 2) delle n^{ple} di numeri $(p_1, p_2, \dots p_n)$, esclusa la disposizione $(0, 0, \dots 0)$ (mod 2), che è impossibile. Ciascuno dei numeri p_i può avere (mod 2) il valore <u>0</u> ovvero <u>1</u>, e il numero delle dette disposizioni è dunque $2^n - 1$. Concludiamo che: <u>di numeri η dotati delle proprietà enunciate ve ne è un numero finito $\leq 2^{n+1} - 2$.</u> Di qui si deduce nuovamente che questi numeri η sono radici dell'unità, poichè ogni potenza η^m di un numero η è ancora un numero η, e la serie illimitata di queste potenze può constare al più di $2^{n+1} - 2$ termini distinti.

Così abbiamo stabilito: <u>Il numero delle radici dell'unità (unità ridotte) contenute in un corpo algebrico di grado n non supera $2^{n+1} - 2$.</u> Si ricordi altresì (pag. 141) che que-

sto numero può superare 2 solo quando il corpo e tutti i suoi corpi coniugati sono immaginarii.

Osserviamo ancora che dalle considerazioni precedenti segue in particolare il teorema di Kronecker (Werke Bd. I. S. 105): Se le radici di un'equazione intera a coefficienti interi, e con primo coefficiente eguale a uno, hanno tutte moduli = 1, esse sono radici della unità.

Fine.

Elenco delle principali opere consultate per la redazione del presente corso.

I) **Bachmann**.- Allgemeine Arithmetik der Zahlenkörper (Leipzig-Teubner-1905).

II) **Cazzaniga**.- Elementi della teoria dei numeri (Padova-Drucker-1903).

III) **Dirichlet-Dedekind**.- Vorlesungen über Zahlentheorie IV Auflage 1894.

III*) id.- Traduzione italiana Faifofer (1881).

IV) **Fubini**.- Lezioni di teoria dei numeri - (Litografia Viretto - Torino - Anno 1916-17).

V) **Hilbert**.- Die Theorie der algebraischen Zahlenkörper (Bericht erstattet der Deutschen-Math.-Vereigung - 4er Band, 1897).

VI) **Landau**.- Handbuch der Lehre von der Vertheilung der Primzahlen (2 volumi - Leipzig-Teubner - 1909).

VII) **Landau**.- Elementare analytische Theorie der algebraischen Zahlen und der Ideale (Leipzig-Teubner-1918).

VIII) Minkowski.- Diophantische Approximationen (Leipzig-Teubner-1907).

IX) Minkowski.- Geometrie der Zahlen (Leipzig-Teubner-1910).

X) Sommer.- Vorlesungen über Zahlentheorie (Leipzig-Teubner-1907).

9

31